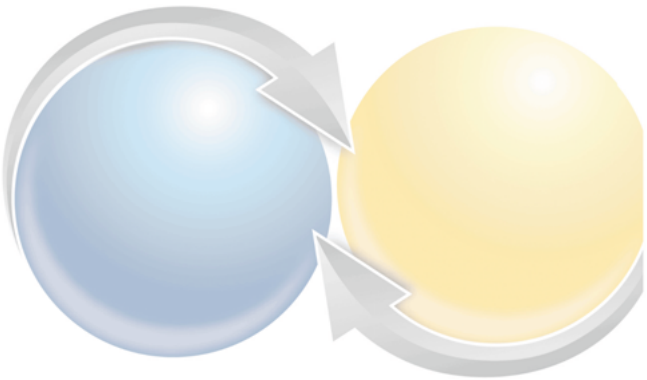
Livelink WCM Server

Installationshandbuch

Dieses Handbuch beschreibt die Installation von Livelink WCM Server. Sie erhalten Informationen zu folgenden Themen:

- Datenbank einrichten
- LDAP-System einrichten
- WCM-System sowie einzelne Komponenten installieren und deinstallieren
- Webserver einrichten
- Upgrade eines WCM-Systems durchführen



OPEN TEXT CORPORATION

Great Minds Working Together™

Copyright 2006 Open Text Corporation

Das Copyright an diesen Unterlagen und der dazugehörigen Software gehört ohne Einschränkungen der Open Text Corporation. Diese Unterlagen und die dazugehörige Software dürfen ohne die ausdrückliche, schriftliche Genehmigung der Open Text Corporation weder ganz noch teilweise kopiert werden.

Die Open Text Corporation ist Eigentümer der Warenzeichen Open Text, 'Great Minds Working Together', Livelink, MeetingZone u.a.; diese Liste ist nicht vollständig. Andere in der Dokumentation erwähnte Warenzeichen sind Eigentum des jeweiligen Unternehmens und werden nur zum Zweck der Identifizierung der Produkte und Unternehmen verwendet. Alle Rechte vorbehalten.

Für die in diesem Dokument beschriebene Software der Open Text Corporation gelten bestimmte Gewährleistungen und Einschränkungen. Informationen zu diesen Gewährleistungen und Einschränkungen erhalten Sie in dem Lizenzvertrag, der zwischen dem Lizenznehmer und der Open Text Corporation geschlossen wurde.

Kontaktadresse:

Unternehmenshauptsitz
Open Text Corporation
275 Frank Tompa Drive,
Waterloo, Ontario
N2L 0A1
Kanada

Telefon: +1 519 888-7111

Wenn Sie Abonnent des Customer Assistance Program sind oder weitere Informationen zum Kundendienstprogramm wünschen, wenden Sie sich an den Kundendienst von Open Text Corporation unter support@opentext.com oder per Telefon unter +1 (800) 540-7292 oder +1 (519) 888-9933. Unser Kundendienst ist Montag-Freitag von 8:30 Uhr bis 20:00 Uhr (EST) erreichbar.

Wenn Sie zu dieser Dokumentation Anmerkungen haben oder Vorschläge machen möchten, senden Sie eine E-Mail-Nachricht an documentation@opentext.com.

Weitere Informationen zu den Produkten und Dienstleistungen der Open Text Corporation finden Sie auf unserer Homepage unter http://www.opentext.com.

© 2006 IXOS SOFTWARE AG

Werner-v.-Siemens-Ring 20
85630 Grasbrunn, Deutschland

Tel.: +49 (89) 4629-0
Fax: +49 (89) 4629-1199
E-Mail: office@ixos.de
Internet: http://www.ixos.com

Alle Rechte vorbehalten. Einschließlich solche, die die Reproduktion, das Kopieren oder eine andere Verwendung oder Übermittlung der Inhalte dieses Dokumentes oder Teile davon betreffen. Kein Teil dieser Publikation darf, egal in welcher Form, ohne die schriftliche

Zustimmung der IXOS SOFTWARE AG reproduziert, an Dritte übermittelt, unter Einsatz elektronischer Retrieval-Systeme verarbeitet, kopiert, verteilt oder für öffentliche Vorführungen verwendet werden. IXOS behält sich das Recht vor, Aktualisierungen und Änderungen der Inhalte vorzunehmen. Sämtliche Daten, die auf Bildschirmfotos (screenshots) sichtbar sind, dienen lediglich als Beispiel zur Demonstration der Software. Für den Inhalt dieser Daten übernimmt IXOS keine Gewähr. Dieses Produkt beinhaltet Software, die im Rahmen des Projekts OpenSSL für den Gebrauch im OpenSSL Toolkit (http://www.openssl.org/) bzw. die durch die Apache Software Foundation (http://www.apache.org/) entwickelt wurde.

Marken IXOS: IXOS SOFTWARE AG.

SAP®, R/3® und SAP ArchiveLink® sind eingetragene Marken der SAP AG.

Microsoft®, Microsoft Windows NT® und die Namen weiterer Microsoft-Produkte sind eingetragene Marken der Microsoft Corporation.

Acrobat Reader Copyright © 1987 Adobe Systems Incorporated. Alle Rechte vorbehalten. Adobe und Acrobat sind Marken von Adobe Systems Incorporated, die in bestimmten Rechtsbereichen registriert sein können.

Siebel® ist eingetragene Marke der Siebel Systems, Inc.

Sonstige Produktnamen werden nur zur Identifikation der Produkte verwendet und können eingetragene Marken der entsprechenden Hersteller sein.

Copyright © 2006 Gauss Interprise AG Hamburg, Gauss Interprise, Inc. Irvine, California. Alle Rechte weltweit vorbehalten.

Dieses Dokument sowie die zugehörige Software sind Eigentum der Gauss Interprise AG oder ihrer Zulieferer und durch Gesetze zum Schutze des Urheberrechts und andere Gesetze geschützt. Sie werden unter einer Lizenz vertrieben, durch welche die Nutzung, Reproduktion, Vertrieb und Dekompilierung eingeschränkt wird. Weder der Erhalt noch der Besitz dieses Dokumentes ermächtigt Sie, dessen Inhalte ganz oder teilweise auf Papier, elektronisch oder einem anderen Medium zu reproduzieren, weiterzugeben oder anderen den Zugang darauf zu ermöglichen. Kein Teil dieses Dokumentes darf in irgendeiner Form und Weise ohne vorherige schriftliche Zustimmung der Gauss Interprise AG oder Gauss Interprise, Inc. reproduziert werden.

Darüber hinaus gelten für diese Dokumentation die Bestimmungen des Softwarelizenzvertrags.

Alle Warenzeichen oder Handelsmarken, die in diesem Dokument erwähnt wurden, sind Eigentum der entsprechenden Firmen.

http://www.opentext.com/bridging/gauss.html

Programmversion: Livelink Web Content Management Server™ (Content Server) 9.5.1

Dokumentenversion: De-01

Erscheinungsdatum: Mai 2006

Inhaltsverzeichnis

Abbildungsverzeichnis **6**

Tabellenverzeichnis **8**

Kapitel 1 Einleitung **11**

1.1 Vorgehen bei der Installation 11

1.2 Installationsvoraussetzungen 14

1.3 Hinweise zu dieser Dokumentation 16

1.4 Typographische Konventionen 19

Kapitel 2 RDBMS einrichten **21**

2.1 Oracle konfigurieren 22

2.2 MS SQL Server 2000 konfigurieren 31

Kapitel 3 LDAP-Verzeichnisdienst einrichten **35**

3.1 Konzept der Sammelgruppen und Sammelrollen 38

3.2 Zusätzliche Objektklassen und Attribute einrichten 40

3.3 LDAP-Bindeprofil und WCM-Administrator einrichten 56

3.4 Hinweise zur Verwendung mehrerer LDAP-Server 59

3.5 SSL-Verbindung zum LDAP-Server verwenden 64

Kapitel 4 Installation von Livelink WCM Server **71**

4.1 Neues WCM-System installieren (Minimalsystem) 72

4.2 WCM-System benutzerdefiniert installieren 114

4.3 Neue Server hinzufügen 118

4.4 Admin-Client installieren 122

4.5 Lizenz erneuern 124

4.6 Verzeichnisstruktur nach der Installation 126
4.7 WCM-System deinstallieren 130
4.8 Installation und Deinstallation über die Konsole steuern 135
4.9 Server starten und stoppen 162
4.10 Protokoll- und Fehlerdateien 174

Kapitel 5 Webserver einrichten 177
5.1 Szenario 1 – Apache 2 mit Tomcat 180
5.2 Szenario 2 – BEA WebLogic 8.1 183
5.3 Szenario 3 – MS Internet Information Server mit Resin 185
5.4 Das Precompile-Skript 202
5.5 Secure Access konfigurieren 203

Kapitel 6 Upgrade von Livelink WCM Server 227
6.1 Upgrade über die grafische Oberfläche 227
6.2 Upgrade über die Konsole 236
6.3 Notwendige Nacharbeiten nach dem Upgrade 240

Anhang A Produktspezifische Hinweise für LDAP-Verzeichnisdienste 245
A.1 Microsoft Active Directory 246
A.2 Novell eDirectory (NDS) 252
A.3 Sun ONE Directory Server 257
A.4 OpenLDAP 261

Glossar 267

Index 279

Abbildungsverzeichnis

Abb. 1 –	Einstellungen des Datenbank-Servers (SQL Server)	32
Abb. 2 –	Verwendung mehrerer LDAP-Server	60
Abb. 3 –	Nutzung eines LDAP-Servers für mehrere WCM-Systeme	62
Abb. 4 –	Installationsmöglichkeiten im Überblick	71
Abb. 5 –	Optionen beim Installationsvorgang	76
Abb. 6 –	Optionen für die Lizenzverwaltung festlegen	77
Abb. 7 –	Parameter des Administrationsservers	79
Abb. 8 –	Parameter der zu benutzenden Datenbank	82
Abb. 9 –	Parameter des zu benutzenden Livelink-System	86
Abb. 10 –	Parameter des zu benutzenden LDAP-Verzeichnisdienstes	88
Abb. 11 –	WCM-spezifische LDAP-Parameter	91
Abb. 12 –	WCM-Administrator einrichten	94
Abb. 13 –	Installationsvarianten	96
Abb. 14 –	Dialog zum Einrichten der Server	97
Abb. 15 –	Webanwendung für einen Content-Server erzeugen	101
Abb. 16 –	Installation eines Content Miner-Suchservers	106
Abb. 17 –	Installation eines Lucene-Suchservers	108
Abb. 18 –	Installation eines Livelink-Suchservers	111
Abb. 19 –	Auswahl der zu entfernenden Komponenten	133
Abb. 20 –	URL-Mapping in IIS	187
Abb. 21 –	IIS-Konfiguration für Base-Authentifizierung mit anonymem Zugang	194
Abb. 22 –	VIPSecure.dll als ISAPI-Filter konfigurieren (IIS)	196
Abb. 23 –	IIS-Konfiguration für Base-Authentifizierung mit Name und Passwort	198
Abb. 24 –	Konfiguration von IIS für NTLM-Authentifizierung	201
Abb. 25 –	Upgrade der Version durchführen	230

Abb. 26 – Upgrade der Datenhaltung durchführen 234
Abb. 27 – Für das Upgrade ausgewählte Datenhaltungen 235

Tabellenverzeichnis

Tabelle 1 – Werte für die Oracle-Datenbankinstanzen 23
Tabelle 2 – OIDs der LDAP-Objektklassen für Livelink WCM Server 44
Tabelle 3 – OIDs der LDAP-Attribute für Livelink WCM Server 44
Tabelle 4 – Angaben im Abschnitt `<mappings>` 46
Tabelle 5 – Tags zum Steuern der Les- und Schreibbarkeit von LDAP-Attributen 52
Tabelle 6 – Inverse LDAP-Attribute für die Klasse `vipUser` 55
Tabelle 7 – Beispielkonfiguration für separate LDAP-Objektklassen und -attribute 64
Tabelle 8 – Parameter für Keytool 67
Tabelle 9 – Angaben im Abschnitt `<license>` 139
Tabelle 10 – Angaben im Abschnitt `<common>` 140
Tabelle 11 – Angaben im Abschnitt `<admin>` 142
Tabelle 12 – Angaben im Abschnitt `<server>` 144
Tabelle 13 – Angaben im Abschnitt `<contentminer_server>` 148
Tabelle 14 – Angaben im Abschnitt `<lucene_server>` 149
Tabelle 15 – Angaben im Abschnitt `<livelink_search-server>` 151
Tabelle 16 – Angaben im Abschnitt `<rdbms>` 153
Tabelle 17 – Angaben im Abschnitt `<livelink>` 155
Tabelle 18 – Angaben im Abschnitt `<ldap>` 157
Tabelle 19 – Parameter in den Startskripten der Server 166
Tabelle 20 – Parameter in den Stoppskripten der Server 169
Tabelle 21 – Loglevels von Secure Access 216
Tabelle 22 – Angaben im Abschnitt `<update_vip>` 237
Tabelle 23 – Angaben im Abschnitt `<update_rdbms>` 239
Tabelle 24 – WCM-Attribute für die Klasse `vip` (Active Directory) 248
Tabelle 25 – WCM-Attribute für die Klasse `vipUser` (Active Directory) 249

Tabelle 26 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (Active Directory) 250
Tabelle 27 – WCM-Attribute für die Klasse `vip` (NDS) 254
Tabelle 28 – WCM-Attribute für die Klasse `vipUser` (NDS) 255
Tabelle 29 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (NDS) 257
Tabelle 30 – WCM-Attribute für die Klasse `vip` (Sun ONE) 259
Tabelle 31 – WCM-Attribute für die Klasse `vipUser` (Sun ONE) 260
Tabelle 32 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (Sun ONE) 261
Tabelle 33 – WCM-Attribute für die Klasse `vip` (OpenLDAP) 263
Tabelle 34 – WCM-Attribute für die Klasse `vipUser` (OpenLDAP) 264
Tabelle 35 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (OpenLDAP) 265

KAPITEL 1
Einleitung

Dieses Installationshandbuch beschreibt die Vorgehensweise bei der Installation eines WCM-Systems und geht auf die verschiedenen Installationsvarianten sowie weitere Aspekte ein, die bei der Installation beachtet werden müssen.

1.1 Vorgehen bei der Installation

Zur Einrichtung eines WCM-Systems gehört nicht nur die Installation von Livelink Web Content Management Server™ (kurz: Livelink WCM Server). Für den Betrieb eines Content-Management-Systems sind weitere Komponenten erforderlich, u.a. ein relationales Datenbank-Managementsystem, ein HTTP-Server und eine JSP-Engine.

Vor der Installation von Livelink WCM Server

Abhängig von der IT-Infrastruktur Ihres Unternehmens müssen vor der Installation von Livelink WCM Server andere Softwarekomponenten installiert bzw. für die Verwendung mit Livelink WCM Server konfiguriert werden.

So wird zur Speicherung der Website-Daten und (optional) der Benutzerdaten eine relationale Datenbank benötigt, die vor der Installation von Livelink WCM Server eingerichtet sein muss. Für die Speicherung der Benutzerdaten kann auch auf einen bereits vorhandenen LDAP-Verzeichnisdienst oder eine Livelink-Benutzerverwaltung zugegriffen werden.

- Hinweise zur Installation bzw. Einrichtung des RDBMS finden Sie in Kapitel 2 “RDBMS einrichten”.
- Hinweise zur Anbindung eines LDAP-Verzeichnisdienstes finden Sie in Kapitel 3 “LDAP-Verzeichnisdienst einrichten”.
- Hinweise zur Anbindung einer Livelink-Benutzerverwaltung finden Sie im Livelink-Integrationshandbuch.

Installation von Livelink WCM Server

Die Installation erfolgt über ein separates Programm, mit dem verschiedene Aufgaben erfüllt werden können:

- Installation eines neuen WCM-Systems (siehe Abschnitt 4.1 “Neues WCM-System installieren (Minimalsystem)” ab Seite 72 und Abschnitt 4.2 “WCM-System benutzerdefiniert installieren” ab Seite 114)

> **Hinweis:** Lesen Sie vor der Installation eines WCM-Systems im Livelink WCM Server-Administratorhandbuch das Kapitel “Konzepte”, um Informationen über die Architektur von WCM-Systemen zu erhalten.

- Hinzufügen von Servern zu einem bestehenden WCM-System (siehe Abschnitt 4.3 “Neue Server hinzufügen” auf Seite 118)
- Installation des Admin-Clients (siehe Abschnitt 4.4 “Admin-Client installieren” auf Seite 122)
- Erneuern der Lizenz für Livelink WCM Server (siehe Abschnitt 4.5 “Lizenz erneuern” auf Seite 124)
- vollständige oder teilweise Deinstallation eines WCM-Systems (siehe Abschnitt 4.7 “WCM-System deinstallieren” auf Seite 130)

Die Installation von Livelink WCM Server kann auch im Kommandozeilenmodus erfolgen, siehe dazu Kapitel 4 “Installation und Deinstallation über die Konsole steuern”.

Informationen zu den Installationsprotokollen enthält der Abschnitt 4.10 “Protokoll- und Fehlerdateien” auf Seite 174.

Nach der Installation von Livelink WCM Server

Damit alle Komponenten des WCM-Systems reibungslos funktionieren, müssen nach der Installation von Livelink WCM Server andere Komponenten wie HTTP-Server und JSP-Engine konfiguriert werden. Lesen Sie dazu das Kapitel 5 “Webserver einrichten”.

Informationen zum Starten und Herunterfahren der WCM-Server enthält der Abschnitt 4.9 “Server starten und stoppen” auf Seite 162.

Upgrade von Livelink WCM Server

Das Upgrade eines bestehenden WCM-Systems auf eine neue Programmversion wird mithilfe des Installationsprogramms durchgeführt. Die Umstellung erfolgt in zwei Schritten: Zunächst wird das Upgrade der Version durchgeführt, in einem zweiten Schritt das Upgrade der Datenhaltung.

Informationen zur Durchführung eines Upgrades enthält das Kapitel 6 “Upgrade von Livelink WCM Server”

1.2 Installationsvoraussetzungen

Livelink WCM Server setzt für den Betrieb folgende Komponenten voraus, die vor der Installation zur Verfügung stehen müssen.

> **Hinweis:** Angaben zu den unterstützten Versionen der aufgeführten Softwarekomponenten finden Sie in der Freigabemitteilung.

Java 2 Software Development Kit

Das Java 2 SDK (auch: JDK) wird zum Ausführen der WCM-Serverprogramme benötigt. Da alle WCM-Programme – einschließlich der Installation – vollständig in Java implementiert sind, muss das Java 2 SDK vor der Installation des WCM-Systems verfügbar sein.

HTTP-Server

Für den Zugriff auf die generierten Seiten in der Edit-, QS- und Produktionssicht muss auf den Rechnern, auf denen sich entsprechende WCM-Server befinden, ein HTTP-Server installiert sein (z.B. iPlanet Web Server, Apache HTTP Server, Microsoft Internet Information Server).

Damit Ihr WCM-System die verwalteten Informationen bereitstellen kann, muss der HTTP-Server entsprechend konfiguriert werden. Informationen zur Konfiguration des HTTP-Servers entnehmen Sie bitte der Dokumentation des jeweiligen Herstellers und Kapitel 5 “Webserver einrichten”.

JSP-Engine

Für die Nutzung des Content-Clients, des Content-Clients (Classic), des dynamischen Deployments, der Suchserver sowie von Secure Access, InSite Editing und des Portal Manager API benötigen Sie eine JSP-Engine, die am HTTP-Server angemeldet und eingerichtet werden muss.

Informationen zur Konfiguration der JSP-Engine sind in der Dokumentation des jeweiligen Herstellers enthalten. Hinweise zur WCM-spezifischen

Konfiguration der JSP-Engine finden Sie in Kapitel 5 “Webserver einrichten”.

Hinweis: Wenn Sie das Portal Manager API unter UNIX betreiben, achten Sie darauf, dass die Anzahl der Datei-Deskriptoren, die dem JSP-Prozess zur Verfügung stehen, mindestens 1024 beträgt.

Mailserver

Das Benachrichtigen von verantwortlichen Personen im WCM-System erfolgt per E-Mail. Aus diesem Grund muss ein Mailserver installiert und konfiguriert sein. Livelink WCM Server nutzt zum Versenden von E-Mails das SMTP-Protokoll, das von den meisten Mailservern unterstützt wird oder über ein entsprechendes Gateway aktiviert werden kann.

Relationales Datenbank-Managementsystem

Für die Speicherung der WCM-Objekte und (optional) der Benutzerdaten benötigen Sie ein externes, relationales Datenbank-Managementsystem (RDBMS). Livelink WCM Server unterstützt die RDBMS Oracle und MS SQL Server 2000. Genaue Informationen zur Konfiguration des RDBMS erhalten Sie in Kapitel 2 “RDBMS einrichten”.

LDAP-Verzeichnisdienst (Directory-Server)

Durch den Einsatz eines LDAP-Verzeichnisdienstes (LDAP = Lightweight Directory Access Protocol) wie z.B. Sun ONE Directory Server, Novell eDirectory und Microsoft Active Directory können bestehende Benutzerverwaltungen eingebunden werden.

Detaillierte Informationen finden Sie in Kapitel 3 “LDAP-Verzeichnisdienst einrichten”.

Optionale Komponenten

Das WCM-System lässt sich um verschiedene Komponenten erweitern:

- Firewalls

  Das WCM-System kann über mehrere physikalische Rechner verteilt werden. Dabei können mehrere Proxy-Content-Server und ein Proxy-Admin-Server vor einer Firewall (außerhalb des Unternehmensnetzes) eingerichtet werden. In diesem Fall müssen die entsprechenden HTTP- bzw. VIPP-Ports der Server freigeschaltet werden.

  Die Installation eines solchen Systems wird beispielhaft in Abschnitt 4.2 “WCM-System benutzerdefiniert installieren” ab Seite 114 beschrieben.

- Serverseitige Anwendungen

  In Verbindung mit Livelink WCM Server lassen sich sämtliche Möglichkeiten der Webtechnologie nutzen wie z. B. Java-Applets, CGI-Skripte, serverseitige Includes (SSI) und Servlets. Zu diesem Zweck sind teilweise Installationen und/oder Konfigurationen des HTTP-Servers bzw. der JSP-Engine nötig. Diese betreffen nicht das WCM-System und erfordern daher keine Änderungen am WCM-System.

1.3 Hinweise zu dieser Dokumentation

Dieses Handbuch beschreibt die Installation von Livelink WCM Server sowie die dazugehörigen Vor- und Nachbereitungen. Die Installation sollte nur von erfahrenen Systemadministratoren durchgeführt werden. Für die Installation eines WCM-Systems sollten Sie fundierte Kenntnisse in den folgenden Bereichen besitzen:

- Installation und Konfiguration eines Webservers (HTTP-Server und JSP-Engine)
- Standardverfahren der Systemverwaltung, z.B. Einrichtung und Pflege von Benutzerverwaltungssystemen, Verzeichnisbäumen und Dateien
- Verwaltung von relationalen Datenbank-Managementsystemen
- Verwaltung von LDAP-Verzeichnisdiensten (optional)

Zusätzlich zum vorliegenden Installationshandbuch können Sie Informationen aus folgenden Quellen beziehen:

- Livelink WCM Server-Administratorhandbuch: Dieses Dokument beschreibt die Konfiguration und Administration eines WCM-Systems aus der Sicht des Administrators.
- Content-Client-Benutzerhandbuch: Dieses Dokument weist Sie ausführlich in alle Aufgaben der redaktionellen Pflege von Websites im WCM-System ein.
- WCM Java API-Programmierhandbuch: Dieses Dokument enthält Informationen über Interfaces, Klassen und Methoden der Java-Programmierschnittstelle (WCM Java API), mit der die Funktionalität der WCM-Server über externe Programme genutzt werden kann.
- Portal Manager API-Programmierhandbuch: Dieses Handbuch enthält u.a. detaillierte Informationen zur Entwicklung dynamischer und personalisierter Websites auf Grundlage des Portal Manager API.
- WCM WebServices-Programmierhandbuch: Dieses Handbuch enthält Informationen zur Nutzung der Funktionen von Livelink WCM Server über Web-Services.
- Online-Hilfe: Die Clients von Livelink WCM Server (Content-Client, Admin-Client und Content Workflow Modeler) verfügen über Online-Hilfen, die zu jedem Zeitpunkt aufgerufen werden können.

Der Inhalt dieses Handbuchs ist folgendermaßen gegliedert:

- Kapitel 2 “RDBMS einrichten” enthält Informationen zur Konfiguration des relationalen Datenbank-Managementsystems, das zusammen mit Livelink WCM Server verwendet wird.
- Kapitel 3 “LDAP-Verzeichnisdienst einrichten” beschreibt die Konfiguration des LDAP-Verzeichnisdienstes
- Kapitel 4 “Installation von Livelink WCM Server” erläutert die Vorgehensweise bei der Installation eines neuen WCM-System und die übrigen Funktionen des WCM-Installationsprogramms.
- Kapitel 5 “Webserver einrichten” beschreibt an einigen Beispielen die Konfiguration von HTTP-Servern und JSP-Engines für Livelink WCM Server.
- Kapitel 6 “Upgrade von Livelink WCM Server” beschreibt die Durchführung eines Upgrades mithilfe des WCM-Installationsprogramms.
- Anhang A “Produktspezifische Hinweise für LDAP-Verzeichnisdienste” enthält produktspezifische Informationen zur Anbindung an verschiedene LDAP-Verzeichnisdienste.

1.4 Typographische Konventionen

Programmelemente u.Ä. werden im Text folgendermaßen hervorgehoben:

Element	Schriftart oder Symbol	Beispiele
Programmoberfläche wie z.B. Menübefehle, Fenster, Dialoge, Feld- und Schaltflächenbezeichnungen	*Menü → Eintrag*	*Datei → Anlegen*
Pfade zu Verzeichnissen, Namen von Dateien und Verzeichnissen	**Laufwerk:\Verzeichnis\Dateiname**	**D:\WCM\admin.bat**

Zitate aus Programmcode oder Konfigurationsdateien	`Code-Zitate`	`<head>`
		`<title>heading </title>`
		`</head>`

Variablen, d.h. Platzhalter für bestimmte Elemente	{Variable}	{WCM-Installationsverzeichnis}

Wichtige **Hinweise** und **Warnungen** stehen in grauen Kästen. Diese Informationen sollten Sie unbedingt lesen, um Fehler bei der Nutzung und Verwaltung von WCM-Systemen sowie Datenverluste zu vermeiden.

KAPITEL 2

RDBMS einrichten

Für den Betrieb von Livelink WCM Server ist ein relationales Datenbank-Managementsystem erforderlich. In der Datenbank werden die Website-Daten und (optional) die Benutzerdaten des WCM-Systems gespeichert. Livelink WCM Server unterstützt die RDBMS Oracle und MS SQL Server 2000.

Für die Nutzung von Livelink WCM Server kann das RDBMS neu installiert oder ein vorhandenes entsprechend konfiguriert werden. Beides muss **vor** der Installation von Livelink WCM Server erfolgen.

Dieses Kapitel enthält Informationen zur WCM-spezifischen Konfiguration des RDBMS:

- "Oracle konfigurieren" ab Seite 22
- "MS SQL Server 2000 konfigurieren" ab Seite 31

Hinweise

- Informationen zu den unterstützten Versionen des RDBMS erhalten Sie in der Freigabemitteilung von Livelink WCM Server.
- Die Installation des RDBMS erfolgt über das Installationsprogramm des jeweiligen Herstellers. Informationen zum Vorgehen bei der Installation erhalten Sie in der Dokumentation des Herstellers.

- Die Konfiguration des RDBMS hängt im hohen Maße von der IT-Infrastruktur Ihres Unternehmens ab, sodass sich hierzu keine allgemein gültigen Aussagen treffen lassen. Wir empfehlen Ihnen, die Datenbank-Architektur in Zusammenarbeit mit der Professional Services Group der Gauss Interprise AG zu entwickeln.

2.1 Oracle konfigurieren

Hinweise

- Das RDBMS und die WCM-Server sollten aus Performance-Gründen nicht auf demselben Rechner installiert sein.
- Die Tabelleninhalte beim Betrieb des WCM-Systems können starken Veränderungen unterliegen. Führen Sie deshalb in regelmäßigen Abständen die Funktion *Statistiken berechnen* auf den WCM-Tabellen aus. Wie oft Sie diese Funktion ausführen, hängt davon ab, wie häufig Veränderungen an den WCM-Tabellen vorgenommen werden (für den Anfang empfiehlt sich eine monatliche Ausführung). Sie sollten die Statistiken berechnen, wenn die Performance des WCM-Systems sinkt.

  Das Berechnen der Statistiken kann komfortabel über das mitgelieferte Oracle-Verwaltungsprogramm “Enterprise Manager Console” erfolgen, das z.B. nach der Installation von Oracle unter Windows über *Start* → *Programme* → *Oracle* → *Enterprise Manager Console* gestartet werden kann. Um die Statistiken zu berechnen, wählen Sie nach der Anmeldung an der Datenbank die Funktion *Extras* → *Datenbank-Werkzeuge* → *Analysieren* → *Statistiken berechnen*.
- Stellen Sie sicher, dass die Version des verwendeten Datenbanktreibers mit der Version der Datenbank übereinstimmt.

Um ein vorhandenes RDBMS zusammen mit Livelink WCM Server zu nutzen, müssen einige Einstellungen im RDBMS angepasst werden. Dazu gehören:

- Datenbankinstanzen (siehe folgenden Abschnitt)
- Nutzung offener Cursor (siehe Abschnitt “Nutzung offener Cursor” auf Seite 25)
- maximale Anzahl von Servern zur Parallelausführung (siehe Abschnitt “Serverprozesse zur Parallelausführung” auf Seite 26)

Außerdem müssen Sie einen Tablespace und einen Benutzer für Livelink WCM Server anlegen (siehe Abschnitt “Datenbankbenutzer und Tablespace in Oracle anlegen” ab Seite 27).

Datenbankinstanz(en) einrichten

Beim Einrichten der Datenbankinstanz(en) müssen bestimmte Parameter angepasst bzw. Konfigurationseinstellungen vorgenommen werden. Geben Sie folgende Werte an:

Tabelle 1 – Werte für die Oracle-Datenbankinstanzen

Parameter	Wert	Änderbar
Register *Speicher* → *Shared Pool*	150 MB	✓
Register *Zeichensätze* → *Datenbank-Zeichensatz*	UTF-8	
Register *Zeichensätze* → *Länderspezifischer Zeichensatz*	UTF-8	
Register *DB-Skalierung* → *Blockgröße*	8 KB	
Register *Archiv* → *Archivelog-Modus*	aktivieren	✓

Parameter	Wert	Änderbar
Schaltfläche *Alle Initialisierungsparameter* → *log_checkpoint_interval*	100000	✓
Schaltfläche *Alle Initialisierungsparameter* → *open_cursors*	1000	✓
Schaltfläche *Alle Initialisierungsparameter* → *parallel_max_servers*	5	✓
Schaltfläche *Alle Initialisierungsparameter* → *processes*	500	✓

Für die übrigen Parameter können die Standardeinstellungen übernommen werden.

Hinweise

- Die Parameter “Datenbank-Zeichensatz” und “Länderspezifischer Zeichensatz” können nachträglich **nicht** mehr geändert werden! Mit der Einstellung “UTF-8” stellen Sie die Datenbank auf Unicode um. Alternativ kann hier auch “ISO 8859” eingestellt werden. Damit ist jedoch kein Unicode in den Metadaten der WCM-Objekte möglich, d.h. beispielsweise auch keine Unterstützung von asiatischen Sprachen. Sie sollten die Datenbank auch auf UTF-8 einstellen, wenn in Ihrer Website Latin-1-Encoding verwendet wird. Der zusätzliche Speicherbedarf für UTF-8-Encoding ist relativ gering. Auf diese Weise vermeiden Sie jedoch eine spätere Migration der Datenbank.
- Beachten Sie die allgemeinen Informationen zur Verwendung von Unicode mit Livelink WCM Server im Livelink WCM Server-Administratorhandbuch (Kapitel “Konzepte”).
- Es empfiehlt sich, die Datenbank in den Archivelog-Modus zu setzen. Dieser Modus erleichtert das Wiederherstellen der Datenbank bei Fehlern. In diesem Modus ist jedoch mit minimalen Performance-Einbußen zu rechnen.

Nutzung offener Cursor

Ein Datenbank-Cursor ist ein Bereich im Arbeitsspeicher der Datenbank, in dem interne Informationen zwischengespeichert werden. Auch Livelink WCM Server öffnet Cursor in der Datenbank. Diese werden vor allem für zwei Zwecke benötigt:

- Jedem Oracle-Statement, das mehr als eine Zeile bearbeitet (sowohl lesend als auch schreibend), wird von der Datenbank ein Cursor zugewiesen. Mithilfe dieses Cursors können Ergebnisse zeilenweise bearbeitet werden. Nach Auswertung der Abfrage durch Livelink WCM Server wird der Cursor geschlossen, d. h. der reservierte Speicher freigegeben.
- Jeder Anweisung, die Livelink WCM Server an die Datenbank schickt (in Form von Prepared Statements), wird ein Cursor zugewiesen. In diesem Fall dient der Cursor der beschleunigten Ausführung der Anweisung.

Livelink WCM Server verursacht durch die verstärkte Nutzung von Prepared Statements eine große Anzahl offener Cursor. Die Verbindungen von Livelink WCM Server zur Datenbank werden in JDBC-Pools verwaltet. Über den Admin-Client können Sie in den Einstellungen von JDBC-Pools die Anzahl der maximal geöffneten Verbindungen festlegen. Jede Verbindung kann die in den *Erweiterten Einstellungen* des Pools angegebene maximale Cursoranzahl öffnen. Wird der Pool von mehreren Servern genutzt, so kann jeder Server die im Pool angegebene maximale Verbindungsanzahl nutzen. Daraus ergibt sich eine sehr hohe, theoretisch mögliche Zahl an offenen Cursorn, die für Livelink WCM Server benötigt werden. Dieser Wert wird jedoch in der Praxis nie erreicht.

Passen Sie den Wert für die Anzahl der offenen Cursor pro Sitzung in der Datenbank entsprechend der Konfiguration Ihres WCM-Systems an (Anzahl der Server und Anzahl von Verbindungen pro JDBC-Pool). Dieser Wert wird nur durch die gegebenen Betriebssystemressourcen begrenzt. Setzen Sie den Parameter “open_cursors” für den Anfang z. B. auf 1000.

Hinweise

- Es empfiehlt sich, einen möglichst großen Wert für die Anzahl der gleichzeitig geöffneten Cursor einzustellen.
- Sollte die festgesetzte Anzahl offener Cursor einmal durch Livelink WCM Server überschritten werden, erzeugt Oracle eine entsprechende Fehlermeldung; die betroffene Aktion im WCM-System schlägt fehl.
- Der Rechner, auf dem die Datenbank installiert ist, muss entsprechend leistungsfähig sein.
- Im Admin-Client können Sie die Anzahl der maximal offenen Cursor pro JDBC-Pool angeben. Die dort eingestellten Werte sind bereits für Livelink WCM Server optimiert und sollten nur in Zusammenarbeit mit der Gauss Interprise AG geändert werden.

  Falls wiederholt Fehlermeldungen durch Oracle oder Livelink WCM Server über eine unzureichende Cursoranzahl auftreten, wenden Sie sich bitte an den Technical Support der Gauss Interprise AG.

Serverprozesse zur Parallelausführung

Die für eine Datenbankinstanz maximale Anzahl von Servern zur Parallelausführung bzw. von Prozessen zur parallelen Wiederherstellung wird über den Initialisierungsparameter “parallel_max_servers” bestimmt. Setzen Sie den Parameterwert auf 5.

Je nach Bedarf wird die Anzahl von Abfrageservern, die der Datenbankinstanz beim Hochfahren zugewiesen werden, auf diese maximale Anzahl erhöht.

Jede Serverinstanz kann – je nach Leistungsfähigkeit des Rechners – eine bestimmte Anzahl von Prozessen haben. Diese Anzahl wird über den Parameter “processes” bestimmt, der ebenfalls angepasst werden sollte (Wert = 500).

Datenbankbenutzer und Tablespace in Oracle anlegen

In der Datenbank werden die Daten des WCM-Systems in einem so genannten Tablespace (Tabellenbereich) verwaltet. Nach der Konfiguration des RDBMS müssen Sie daher einen Tabellenbereich und einen Datenbankbenutzer für das WCM-System anlegen.

Hinweise:

Wenn mehrere WCM-Server ihre Daten in einer Datenbank und insbesondere in einem Tablespace speichern, können daraus Engpässe in den Systemressourcen des Datenbankrechners resultieren. Aus diesem Grund sollte jedes WCM-System auf eine eigene Datenbank zugreifen. Bei mehreren Installationen des WCM-Systems muss für jede Installation ein eigener Tabellenbereich und ein separater Datenbankbenutzer eingerichtet werden.

Die Proxy-Content-Server des WCM-Systems können ebenfalls so konfiguriert werden, dass sie über eine eigene Datenhaltung verfügen. Auf diese Weise wird die Datenbank des Master-Content-Servers weniger beansprucht.

Das Erzeugen des Tablespaces und Anlegen des Datenbankbenutzers kann über die Enterprise Manager Console oder per SQL-Befehl erfolgen. Richten Sie in jedem Fall zuerst den Tabellenbereich und anschließend den Datenbankbenutzer ein.

Größe des Tablespaces

Der Tablespace für die WCM-Daten sollte mindestens 500 MB groß sein. Der Name ist frei wählbar. Außerdem ist ein Temporary Tablespace erforderlich, der mindestens eine Größe von 70 MB haben muss. Die benötigte Größe des Tablespaces kann stark variieren und wird vor allem durch folgende Faktoren beeinflusst:

- Größe des Inhalts, der mit Livelink WCM Server verwaltet wird
- Grad der Verlinkung zwischen den Objekten
- Häufigkeit der Änderung an Objekten und die daraus resultierende Anzahl an Objektversionen
- Anzahl der archivierten Versionen (diese kann über das Dienstprogramm “Datenbank-Bereinigung” gesteuert werden, siehe Livelink WCM Server-Administratorhandbuch)

Berechtigungen und Zuordnungen des Benutzers

Der Datenbankbenutzer für das WCM-System sollte über die Rollen “CONNECT” und “RESOURCE” verfügen.

Wenn Sie die genannten Rollen nicht vergeben möchten, dann ordnen Sie dem Benutzer folgende Systemberechtigungen zu:

- CREATE TABLE
- CREATE TRIGGER
- CREATE PROCEDURE
- CREATE SESSION

Zusätzlich zu diesen Berechtigungen benötigt der Benutzer die Berechtigung UNLIMITED TABLESPACE oder entsprechende Quoten auf dem Tablespace.

Weisen Sie dem Datenbankbenutzer den WCM-Tablespace als “Default Tablespace” und den Temporary Tablespace als “Temporary Tablespace” zu.

Tablespace und Benutzer einrichten

Das Einrichten von Tabellenbereich und Datenbankbenutzer kann über die Enterprise Manager Console erfolgen. Weitere Informationen finden Sie in der Online-Hilfe der Enterprise Manager Console.

So richten Sie den Tabellenbereich und den Datenbankbenutzer per SQL-Befehl ein:

1. Starten Sie das Datenbank-Frontend SQL Plus. Die Startdatei für Windows **sqlplusw.exe** befindet sich im Verzeichnis **{Oracle-Installationsverzeichnis}\bin**.
2. Melden Sie sich mit der Benutzerkennung des Systemverwalters an.

   Geben Sie das entsprechende Passwort ein. Im Feld *Host-Zeichenfolge* sind folgende Einträge möglich:

   - Das Feld bleibt leer: Es wird eine Datenbank auf dem lokalen Rechner gesucht.
   - Name der Datenbank (z.B. “wcmdb”): Eine Datenbank mit diesem Namen wird auf dem lokalen Rechner gesucht.
   - {Datenbankname}_{Name des Datenbankhosts}.{Domäne}, z.B. wcmdb_dbserver.company.example: Eine Datenbank mit diesem Namen wird auf dem angegebenen Rechner gesucht.

Die SQL-Befehle zum Einrichten des Tabellenbereichs und Anlegen des Datenbankbenutzers stellen sich beispielhaft wie folgt dar:

```
SQL> CREATE TABLESPACE wcmspace
2    DATAFILE '{Oracle-Installationsverzeichnis}\oradata\
                {Datenbankname}\wcmspace.ora'
3    SIZE 500M
4    REUSE
5    AUTOEXTEND ON;

Tablespace wurde angelegt.

SQL> CREATE USER wcmuser
2    IDENTIFIED BY wcm123
3    DEFAULT TABLESPACE wcmspace
4    TEMPORARY TABLESPACE temp;

Benutzer wurde angelegt.

SQL> GRANT connect TO wcmuser;

Benutzerzugriff (Grant) wurde erteilt.

SQL> GRANT resource TO wcmuser;

Benutzerzugriff (Grant) wurde erteilt.

SQL>
```

2.2 MS SQL Server 2000 konfigurieren

Bei der Installation von Livelink WCM Server müssen Sie einen JDBC-Treiber für MS SQL Server 2000 angeben (siehe Abschnitt “Parameter des RDBMS einstellen” auf Seite 82). Informationen zu den unterstützten JDBC-Treibern erhalten Sie in der Freigabemitteilung von Livelink WCM Server.

Im Folgenden werden die Konfigurationsänderungen beschrieben, die an einer bestehenden Installation von MS SQL Server 2000 vorgenommen werden müssen.

> **Hinweis:** Wegen des restriktiven Sperrmechanismus von MS SQL Server empfiehlt es sich, für den Master-Content-Server und die Proxy-Content-Server getrennte Datenbanken einzurichten. Auf diese Weise stellen Sie sicher, dass lesende Zugriffe der Proxy-Content-Server nicht durch Aktionen blockiert werden, die auf dem Master-Content-Server ausgeführt werden.

Datenbank und Benutzer für Livelink WCM Server anlegen

Für die Daten des WCM-Systems sollte im RDBMS eine separate Datenbank angelegt werden.

Legen Sie außerdem einen separaten Benutzer für Livelink WCM Server an. Dieser Benutzer muss der für Livelink WCM Server angelegten Datenbank zugeordnet werden und mindestens zu folgenden Gruppen bzw. Rollen gehören:

- Server Role: Public
- Gruppe: db_ddladmin

Der Benutzer muss über die SQL Server-Authentifizierung angemeldet werden können, d. h. über die Benutzerverwaltung der Datenbank angelegt worden sein. Eine Windows-Authentifizierung ist über die JDBC-Treiber für MS SQL Server nicht möglich.

Dieser Benutzer wird bei der Installation von Livelink WCM Server als Eigentümer der Datenbank angegeben, siehe Abschnitt “Parameter des RDBMS einstellen” auf Seite 82.

Eigenschaften der Datenbank

In der Datenbank muss als Authentifizierungsmethode *Authentication SQLServer & Windows* eingestellt werden.

Außerdem muss die Datenbank verschachtelte Trigger zulassen. Aktivieren Sie dazu in den Eigenschaften des Datenbank-Servers auf dem Register *Server Settings* das Kontrollkästchen *Allow triggers to be fired which fire other triggers (nested triggers)*.

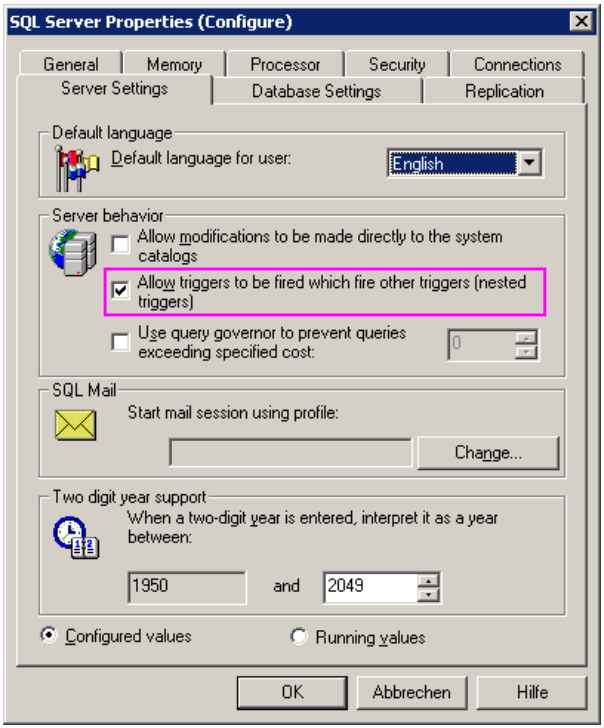


Abb. 1 – Einstellungen des Datenbank-Servers (SQL Server)

KAPITEL 3

LDAP-Verzeichnisdienst einrichten

Alternativ zu einem RDBMS oder Livelink können die Angaben zu Benutzern, Gruppen und Rollen in einem LDAP-Verzeichnisdienst gespeichert werden. In diesem Kapitel wird beschrieben, welche Vorbereitungen für die Nutzung eines LDAP-Verzeichnisdienstes mit Livelink WCM Server erforderlich sind.

Livelink WCM Server kann folgende WCM-Informationen aus dem Verzeichnisdienst nutzen und dort speichern:

- Benutzer mit Name, Benutzerkennung, Passwort, Mailadresse, Sprache und Stellvertreter
- Gruppen mit Name, Mailadresse und zugeordneten Benutzern (statische Gruppen)
- Rollen mit Name, Mailadresse und zugeordneten Benutzern (statische Rollen)
- den Benutzern, Gruppen und Rollen zugeordnete Websites und Funktionsbereiche
- Standard-Objektrechte der Benutzer, Gruppen und Rollen

Hinweise für den LDAP-Zugriff

- Die Konfiguration des LDAP-Verzeichnisdienstes hängt im hohen Maße von der IT-Infrastruktur Ihres Unternehmens ab. Hier wird daher keine detaillierte Anleitung zur Einrichtung des LDAP-Verzeichnisdienstes gegeben, sondern nur die grundsätzliche Konfiguration beschrieben. Wir empfehlen Ihnen, die LDAP-Architektur in Zusammenarbeit mit der Professional Services Group der Gauss Interprise AG zu entwickeln.
- Werden in dem LDAP-Verzeichnisdienst viele Benutzer mit zahlreichen Attributen verwaltet, von denen nur ein Teil auf das WCM-System zugreifen soll und bei denen auch nur ein Teil der Attribute WCM-relevant sind, empfehlen wir, diese Benutzer mit den WCM-relevanten Attributen in ein separates Verzeichnis auszulagern (z. B. über den Replikationsmechanismus des LDAP-Verzeichnisdienstes). Auf diese Weise ist es möglich, den Zugriff auf das WCM-System zu beschleunigen (siehe Abschnitt “LDAP-Abfragen beschleunigen” auf Seite 54).
- Kennungen von WCM-Benutzern dürfen nur folgende Zeichen enthalten: a–z, A–Z und 0–9 (ASCII 7 Bit) sowie - (Bindestrich), _ (Unterstrich), . (Punkt), \ (Backslash = linksseitiger Schrägstrich) und & (kaufmännisches UND).
- WCM-Benutzer müssen eindeutige Kennungen besitzen. Auch die Namen von Gruppen und Rollen müssen eindeutig sein. Im WCM-System wird bei der Schreibweise von Benutzerkennungen, Gruppen- und Rollennamen zwischen Groß- und Kleinschreibung unterschieden.
- Im Admin-Client des WCM-Systems wird die hierarchische Struktur des LDAP-Verzeichnisdienstes nicht abgebildet. Die Benutzer werden in einer flachen Liste angezeigt. Die LDAP-Position wird jedoch als eine Eigenschaft des Benutzers im Admin-Client angezeigt.

Unterstützte LDAP-Server

Angaben zu den unterstützten LDAP-Servern finden Sie in der Freigabemitteilung von Livelink WCM Server.

LDAP-Verzeichnisdienst für Livelink WCM Server konfigurieren

Um den Zugriff von Livelink WCM Server auf den LDAP-Verzeichnisdienst zu ermöglichen, sind verschiedene Vorbereitungen erforderlich:

1. Einrichten von WCM-Objektklassen und Attributen in LDAP (siehe Abschnitt “Zusätzliche Objektklassen und Attribute einrichten” ab Seite 40)
2. Einrichten der LDAP-Verbindung für Livelink WCM Server und des WCM-Administrators im LDAP-Verzeichnisdienst (siehe Abschnitt 3.3 “LDAP-Bindeprofil und WCM-Administrator einrichten” ab Seite 56)

Mehrere LDAP-Server verwenden

Wenn Sie Benutzern, Gruppen oder Rollen, die in verschiedenen LDAP-Servern verwaltet werden, Zugriff auf das WCM-System ermöglichen möchten, lesen Sie bitte die Informationen im Abschnitt 3.4 “Hinweise zur Verwendung mehrerer LDAP-Server” auf Seite 59.

Dort finden Sie auch Informationen zur Nutzung eines LDAP-Verzeichnisdienstes für mehrere WCM-Systeme.

SSL für die Verbindung zum LDAP-Server verwenden

Die Verbindung des WCM-Systems zum LDAP-Server kann über sichere Verbindungen (SSL = Secure Socket Layer) erfolgen. Informationen dazu finden Sie im Abschnitt 3.5 “SSL-Verbindung zum LDAP-Server verwenden” auf Seite 64.

3.1 Konzept der Sammelgruppen und Sammelrollen

In diesem Abschnitt wird Ihnen ein erweitertes Konzept der LDAP-Gruppen und -Rollen vorgestellt. Dieses Konzept ist proprietär und nicht Bestandteil des LDAP-Standards. Livelink WCM Server unterscheidet zwei Arten von Gruppen und Rollen:

- Standardgruppen und -rollen
- Sammelgruppen und -rollen

Standardgruppen und -rollen

Den Standardgruppen und -rollen sind die Benutzer über das LDAP-Attribut `member` zugeordnet.

Sammelgruppen und -rollen

Sammelgruppen und -rollen basieren auf den Organisationsstrukturen, die im LDAP-Verzeichnisdienst abgebildet sind. In Sammelgruppen/-rollen können alle Typen von WCM-Principals (Benutzer, Gruppen, Rollen) enthalten sein.

Folgende Benutzer sind einer Sammelgruppe/-rolle zugeordnet:

- Alle Benutzer, die der Sammelgruppe/-rolle über das LDAP-Attribut `member` zugeordnet sind (entspricht dem Verhalten bei Standardgruppen/-rollen). Hierbei handelt es sich um eine explizite Zuordnung.
- Alle unterhalb der Sammelgruppe/-rolle im LDAP-Baum befindlichen WCM-Benutzer. Hierbei handelt es sich um eine implizite Zuordnung.
- Alle über das LDAP-Attribut `member` referenzierten Benutzer aus Standardgruppen/-rollen, die sich im LDAP-Baum unterhalb der Sammelgruppe/-rolle befinden. Hierbei handelt es sich um eine implizite Zuordnung.

Hinweise zu Sammelgruppen/-rollen

- Die Benutzer, die der Sammelgruppe/-rolle implizit zugeordnet sind, sind zwar im Admin-Client sichtbar; Sie können die **impliziten** Zuordnungen jedoch nicht über den Admin-Client oder das WCM Java API bearbeiten. Änderungen müssen direkt im LDAP-Verzeichnisdienst vorgenommen werden.
- In Livelink WCM Server wird nicht sichtbar zwischen implizit und explizit zugeordneten Benutzern unterschieden. Diese Information finden Sie im LDAP-Verzeichnisdienst.
- Es kann kein Alias benutzt werden, um die Beziehung “unterhalb der Sammelgruppe/-rolle im LDAP-Baum” herzustellen.

Option *Sammelgruppen/-rollen*

Mithilfe der Option *Sammelgruppen/-rollen* in den Einstellungen des LDAP-Pools können Sie festlegen, dass implizite Zuordnungen von Benutzern zu Gruppen und Rollen im WCM-System berücksichtigt werden. Diese Einstellung steht Ihnen im Installationsprogramm (siehe Abschnitt “Parameter des LDAP-Verzeichnisdienstes einstellen” auf Seite 88) und über den Admin-Client zur Verfügung.

Die vorgenommene Einstellung gilt global für den LDAP-Pool. Wenn Sie in Ihrem WCM-System mehrere LDAP-Pools einrichten, muss sichergestellt sein, dass diese Einstellung identisch ist für Pools, deren LDAP-Kontexte sich überschneiden.

3.2 Zusätzliche Objektklassen und Attribute einrichten

Vor der Installation des WCM-Systems müssen Sie im LDAP-Server zusätzliche Objektklassen und Attribute einrichten, damit Sie Benutzer, Gruppen und Rollen des WCM-Systems auf Grundlage des LDAP-Verzeichnisdienstes verwalten können. Zu diesem Zweck benötigen Sie die base DN (Suchknoten), ein LDAP-Bindeprofil inklusive des Passworts und die LDAP-URL.

Hinweise

- Es findet **kein** Kopieren der Benutzerdaten statt. Die Benutzer werden direkt über den LDAP-Verzeichnisdienst verwaltet. Eine Synchronisation ist daher nicht erforderlich.
- Informationen darüber, wie Sie Objektklassen und Attribute im LDAP-Verzeichnisdienst einrichten, erhalten Sie in der Dokumentation des jeweiligen Produkts.
- Detaillierte Informationen zu den LDAP-Verzeichnisdiensten Microsoft Active Directoy, Novell eDirectory, Sun ONE Directory Server und OpenLDAP finden Sie in Anhang A “Produktspezifische Hinweise für LDAP-Verzeichnisdienste”.

Für die Identifizierung der LDAP-Objektklassen und -Attribute werden so genannte OIDs (Object Identifiers) verwendet. Sie können eigene OIDs entsprechend der Organisation Ihres LDAP-Verzeichnisdienstes nutzen oder die OIDs der Gauss Interprise AG verwenden. Einen Überblick über die OIDs finden Sie in Abschnitt “LDAP-OIDs der Gauss Interprise AG” auf Seite 43.

Objektklassen für Livelink WCM Server

Folgende Objektklassen sind für Livelink WCM Server erforderlich:

- Klasse zu Speicherung der Benutzerinformationen
  Standardname = `vipUser`
- Klasse zur Speicherung der Gruppeninformationen
  Standardname = `vipGroup`
- Klasse zur Speicherung der Rolleninformationen
  Standardname = `vipRole`

Diese Objektklassen sollten von einer gemeinsamen Oberklasse `vip` abgeleitet sein, deren Oberklasse `top` ist. Sie können auch andere Namen für die Objektklassen verwenden. Bei der Installation von Livelink WCM Server und beim späteren Einrichten von Pools für Verbindungen zu einem LDAP-Verzeichnisdienst müssen Sie dann diese Namen angeben, damit die Speicherung der WCM-Benutzerinformationen korrekt vorgenommen werden kann.

Für die WCM-Objektklassen sind folgende WCM-Attribute erforderlich:

Attribute für die Objektklasse `vip`

- `vipAccess` = Erlaubnis für den Zugriff auf das WCM-System
- `vipWebsite` = zugeordnete Websites
- `vipFuncarea` = Funktionsbereiche
- `vipRights` = Standard-Objektrechte
- optional: `vipType` = Principal-Typ (Benutzer, Gruppe oder Rolle)

Attribute für die Objektklasse `vipUser`

- `cn` = common name = Benutzername
- `uid` = unique user ID = Benutzerkennung für das WCM-System

- `email` = E-Mail-Adresse des Benutzers
- `vipLanguage` = Spracheinstellung des Benutzers (locale)
- `vipUserPassword` = Benutzerpasswort in LDAP und für das WCM-System
- `initPassword` = Anzeiger, ob der Benutzer bei der nächsten Anmeldung zur Passwort-Änderung aufgefordert wird
- `trustedLogin` = vertraute Anmeldung ohne Passwort
- `vipSubstitute` = Stellvertreter, “distinguished name” eines WCM-Benutzers
- `hclProfiles` = Profil für den Content-Client
- `vipDomain` = Domäne des Benutzers (bei Verwendung von Secure Access und der Anmeldemethode “ntlm”)

Attribute für die Objektklassen `vipGroup` und `vipRole`

- `cn` = common name = eindeutiger Gruppen- bzw. Rollenname
- `member` = “distinguished names” der zugeordneten Benutzer
- `email` = E-Mail-Adresse der Gruppe bzw. Rolle

Folgende Attribute werden standardmäßig als namensgebende Attribute für den “distinguished name” von Benutzern, Gruppen und Rollen verwendet:

- `uid` der Klasse `vipUser` = eindeutige Benutzerkennung
- `cn` der Klasse `vipGroup` = eindeutiger Gruppenname
- `cn` der Klasse `vipRole` = eindeutiger Rollenname

Hinweise

- Der Wert des namensgebenden Attributs eines WCM-Benutzers **muss** eindeutig sein.

- Mehrwertige “relative distinguished names” (RDN) können von Livelink WCM Server nicht ausgewertet werden.
- Die genaue Vorgehensweise beim Einrichten der Objektklassen und Attribute ist vom verwendeten LDAP-Verzeichnisdienst abhängig. Je nach Produkt müssen die WCM-Attribute außerdem auf LDAP-Attribute gemappt werden (siehe Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45). Beachten Sie deshalb die Informationen zu den unterstützten LDAP-Verzeichnisdiensten in Anhang A “Produktspezifische Hinweise für LDAP-Verzeichnisdienste”.
- Generell gilt für die Arbeit im Admin-Client, dass Attribute, die einen Bestandteil (Namenskomponente) des DN ausmachen, nicht verändert werden dürfen.
- Bei den WCM-Attributen wird zwischen Groß- und Kleinschreibung unterschieden.

LDAP-OIDs der Gauss Interprise AG

Jedes LDAP-Schema ist durch eine weltweit eindeutige OID (Object Identifier) gekennzeichnet. Diese OIDs werden durch eine zentrale Organisation (IANA) vergeben. Eindeutige OIDs sind vor allem bei der Verwendung von SNMP (Simple Network Management Protocol) erforderlich.

Für die Objektklassen und Attribute, die im LDAP-Verzeichnisdienst hinzugefügt werden, können Sie die OIDs der Gauss Interprise AG verwenden oder eigene OIDs registrieren lassen. Die folgenden Tabellen enthalten die OIDs der Gauss Interprise AG.

Die Organisations-OID der Gauss Interprise AG ist 1.3.6.1.4.1.2027. Diese Nummer wird fortgesetzt mit 2.1 für die LDAP-Attribute und mit 2.2 für die LDAP-Objektklassen von Livelink WCM Server. Die einzelnen Attribute und Objektklassen sind in einer flachen Liste registriert.

Tabelle 2 – OIDs der LDAP-Objektklassen für Livelink WCM Server

Objektklasse	OID
vip	1.3.6.1.4.1.2027.2.2.8.1
vipUser	1.3.6.1.4.1.2027.2.2.8.2
vipGroup	1.3.6.1.4.1.2027.2.2.8.3
vipRole	1.3.6.1.4.1.2027.2.2.8.4

Tabelle 3 – OIDs der LDAP-Attribute für Livelink WCM Server

Attribut	OID
vipType	1.3.6.1.4.1.2027.2.1.1
vipAccess	1.3.6.1.4.1.2027.2.1.2
vipRights	1.3.6.1.4.1.2027.2.1.3
vipFuncarea	1.3.6.1.4.1.2027.2.1.4
vipWebsite	1.3.6.1.4.1.2027.2.1.5
vipSubstitute	1.3.6.1.4.1.2027.2.1.6
initPassword	1.3.6.1.4.1.2027.2.1.7
trustedLogin	1.3.6.1.4.1.2027.2.1.8
hclprofiles	1.3.6.1.4.1.2027.2.1.10
vipUserpassword	1.3.6.1.4.1.2027.2.1.11
vipDomain	1.3.6.1.4.1.2027.2.1.12

Attribut	OID
vipSubstituteOf	1.3.6.1.4.1.2027.2.1.13
vipLanguage	1.3.6.1.4.1.2027.2.1.14
vipMemberOf	1.3.6.1.4.1.2027.2.1.15

WCM-Attribute auf LDAP-Attribute mappen

Beim Einrichten der Objektklassen und Attribute im LDAP-Server können folgende Fälle auftreten:

- Existieren einige der oben aufgeführten Attribute bereits im LDAP-Server, können sie den WCM-Klassen einfach zugeordnet werden, wenn sie die richtige Semantik und Syntax aufweisen.
- Existieren einige Attribute bereits im LDAP-Server, die zwar den gleichen Namen, aber ungültige Werte haben, müssen Sie zusätzliche benutzerdefinierte Attribute anlegen.
- Existieren einige Attribute bereits im LDAP-Server, die zwar gültige Werte, aber andere Namen haben, ordnen Sie die benötigten WCM-Attribute den vorhandenen LDAP-Attributen zu. Dies wird als Mapping bezeichnet und im Folgenden beschrieben.

Vor der Installation des WCM-Systems wird das Mappen der Attribute in der Datei **defaults.xml** vorgenommen. Diese Datei befindet sich im Verzeichnis **\installation** auf der WCM-CD und enthält die erforderlichen Parameter für die Installation.

Nach der Installation können Sie die LDAP-Mappings in der Datei **ldapmapping.xml** anpassen, die sich im Verzeichnis **\config** des WCM-Installationsverzeichnisses befindet. Für jeden LDAP-Pool gibt es in dieser Datei einen separaten Abschnitt.

Die folgende Tabelle beschreibt den Abschnitt der Datei **defaults.xml** bzw. **ldapmapping.xml**, in dem die Mappings vorgenommen werden.

Tabelle 4 – Angaben im Abschnitt `<mappings>`

Eintrag in der XML-Datei	Erläuterung

`<CN>`
`<vipattr>cn</vipattr>`
`<ldapattr>cn</ldapattr>`
`</CN>`
	Benutzername bzw. eindeutiger Gruppen- oder Rollenname.
	Hinweis: Wenn Sie dieses Mapping ändern, muss in den Mappings `<LDAP_USER_NAME>`, `<LDAP_GROUP_NAME>` und `<LDAP_ROLE_NAME>` der Wert des Attributs `<ldapattr>` entsprechend angepasst werden.

Eintrag in der XML-Datei	Erläuterung
<LDAP_USER_NAME> <vipattr>userclass.name</vipattr> <ldapattr>cn</ldapattr> <ldapread>false</ldapread> </LDAP_USER_NAME> <LDAP_GROUP_NAME> <vipattr>groupclass.name</vipattr> <ldapattr>cn</ldapattr> <ldapread>false</ldapread> </LDAP_GROUP_NAME> <LDAP_ROLE_NAME> <vipattr>roleclass.name</vipattr> <ldapattr>cn</ldapattr> <ldapread>false</ldapread> </LDAP_ROLE_NAME> <READ_PRINCIPAL_NAME> <vipattr>principal.name</vipattr> <ldapattr>sn</ldapattr> <ldapread>false</ldapread> <ldapwrite>false</ldapwrite> </READ_PRINCIPAL_NAME>	Diese Mappings werden benötigt, damit für Benutzer und Gruppen/Rollen unterschiedliche Attribute für den Namen verwendet werden können. Weitere Informationen finden Sie im Abschnitt “Unterschiedliche Attribute für die Principal-Namen verwenden” auf Seite 52.

Eintrag in der XML-Datei	Erläuterung
<INIT_PASSWORD> <vipattr>initPassword</vipattr> <ldapattr>initPassword</ldapattr> </INIT_PASSWORD>	Anzeiger, ob der Benutzer bei der nächsten Anmeldung zur Passwort-Änderung aufgefordert wird
<LANGUAGE> <vipattr>language</vipattr> <ldapattr>language</ldapattr> </LANGUAGE>	Spracheinstellung des Benutzers
<LDAP_OBJECTCLASS> <vipattr>objectclass</vipattr> <ldapattr>objectClass</ldapattr> </LDAP_OBJECTCLASS>	Typ des LDAP-Eintrags
<VIP_TYPE> <vipattr>viptype</vipattr> <ldapattr>vipType</ldapattr> </VIP_TYPE>	Principal-Typ (Benutzer, Gruppe oder Rolle)
<USER_ID> <vipattr>userid</vipattr> <ldapattr>uid</ldapattr> </USER_ID>	Eindeutige Benutzerkennung für das WCM-System

Eintrag in der XML-Datei	Erläuterung

`<MAIL>`
`<vipattr>email</vipattr>`
`<ldapattr>mail</ldapattr>`
`</MAIL>`
	E-Mail-Adresse des Principals

`<TRUSTED_LOGIN>`
`<vipattr>trustedLogin</vipattr>`
`<ldapattr>trustedLogin</ldapattr>`
`</TRUSTED_LOGIN>`
	Vertraute Anmeldung ohne Passwort

`<USER_PASSWORD>`
`<vipattr>vipUserpassword</vipattr>`
`<ldapattr>userPassword</ldapattr>`
`</USER_PASSWORD>`
	Benutzerpasswort in LDAP und für das WCM-System

`<VIP_ACCESS>`
`<vipattr>vipAccess</vipattr>`
`<ldapattr>vipAccess</ldapattr>`
`</VIP_ACCESS>`
	Erlaubnis für den Zugriff auf das WCM-System

`<VIP_FUNCAREAS>`
`<vipattr>vipFuncarea</vipattr>`
`<ldapattr>vipFuncarea</ldapattr>`
`</VIP_FUNCAREAS>`
	Funktionsbereiche, die dem Principal zugeordnet sind

Eintrag in der XML-Datei	Erläuterung

`<VIP_MEMBERS>`
`<vipattr>member</vipattr>`
`<ldapattr>member</ldapattr>`
`</VIP_MEMBERS>`
	“distinguished names” der Benutzer, die der Gruppe oder Rolle zugeordnet sind

`<VIP_RIGHTS>`
`<vipattr>vipRights</vipattr>`
`<ldapattr>vipRights</ldapattr>`
`</VIP_RIGHTS>`
	Standard-Objektrechte, über die der Principal verfügt

`<VIP_SUBSTITUTE>`
`<vipattr>vipSubstitute</vipattr>`
`<ldapattr>vipSubstitute</ldapattr>`
`</VIP_SUBSTITUTE>`
	Stellvertreter, “distinguished name” eines WCM-Benutzers

`<VIP_WEBSITES>`
`<vipattr>vipWebsite</vipattr>`
`<ldapattr>vipWebsite</ldapattr>`
`</VIP_WEBSITES>`
	Websites, die dem Principal zugeordnet sind

`<HCL_PROFILES>`
`<vipattr>hclProfiles</vipattr>`
`<ldapattr>hclProfiles</ldapattr>`
`</HCL_PROFILES>`
	Profil des Benutzers im Content-Client

Eintrag in der XML-Datei	Erläuterung
<VIP_DOMAINS> <vipattr>vipDomain</vipattr> <ldapattr>vipDomain</ldapattr> </VIP_DOMAINS>	Domäne des Benutzers (bei Verwendung von Secure Access und der Anmeldemethode “ntlm”)

Lesbarkeit und Schreibbarkeit der LDAP-Attribute steuern

Jeder Eintrag im Abschnitt `<mappings>` kann um die Tags `<ldapread>` und `<ldapwrite>` erweitert werden. Mithilfe dieser Tags steuern Sie, ob die Attributwerte aus dem LDAP-Server gelesen und bei Änderungen wieder im LDAP-Server gespeichert werden können. Diese Tags können Sie nutzen, um den Lese- und/oder Schreibschutz von LDAP-Attributen auf das WCM-System zu übertragen (z.B. für Passwörter).

Hinweise:

Der Admin-Client zeigt nicht an, ob Attribute lesbar und/oder schreibbar sind. Diese Informationen sind nur in der Mapping-Datei enthalten.

Für Attribute, bei denen das Tag `<ldapread>` den Wert `false` hat (die also nicht aus dem LDAP-Server gelesen werden) werden im WCM-System keine Standardwerte gesetzt.

Beispiel

```
<MAIL>
      <vipattr>email</vipattr>
      <ldapattr>mail</ldapattr>
      <ldapread>true</ldapread>
      <ldapwrite>false</ldapwrite>
</MAIL>
```

Die folgende Tabelle veranschaulicht die Kombinationsmöglichkeiten dieser beiden Tags.

Tabelle 5 – Tags zum Steuern der Les- und Schreibbarkeit von LDAP-Attributen

Wert von <ldapread>	Wert von <ldapwrite>	Erklärung
true	true	Standardeinstellung (muss nicht explizit in der Mapping-Datei gesetzt werden) Die Attributwerte können von Livelink WCM Server gelesen und bei Änderungen im LDAP-Verzeichnisdienst gespeichert werden.
true	false	Die Attributwerte können von Livelink WCM Server gelesen werden. Werden sie im WCM-System geändert, können die geänderten Werte jedoch nicht im LDAP-Verzeichnisdienst gespeichert werden. Änderungen der Attributwerte sind nur direkt im LDAP-Verzeichnisdienst möglich.
false	true	Die Attributwerte werden nicht von Livelink WCM Server gelesen. Änderungen können jedoch gespeichert werden.
false	false	Weder Lesen noch Schreiben der Attributwerte ist möglich.

Unterschiedliche Attribute für die Principal-Namen verwenden

Standardmäßig wird für den Namen von Benutzer-Einträgen und Gruppen/Rollen-Einträgen das Attribute CN verwendet. Sie können jedoch auch unterschiedliche Attribute verwenden z. B. für Benutzer das Attribut CN und für Gruppen/Rollen das Attribut SN. Für diesen Fall werden die folgenden Mappings benötigt:

- <LDAP_USER_NAME>, <LDAP_GROUP_NAME>, <LDAP_ROLE_NAME>

  Diese Mappings werden für die Suche und den Schreibzugriff verwendet. Der Lesezugriff muss **immer** ausgeschaltet sein. Der Wert des Attributs <ldapattr> muss für das Gruppen- und das Rollen-Mapping auf den gewünschten Wert gesetzt werden (z.B. sn)

- <READ_PRINCIPAL_NAME>

  Wenn Sie für Benutzer und Gruppen/Rollen verschiedene Attribute für den Namen zu verwenden, muss der Lesezugriff eingeschaltet sein und das Attribut <ldapattr> auf den entsprechenden Wert gesetzt werden (z.B. sn).

Beispiel

Für die Benutzernamen möchten Sie das Attribut fullname, für Gruppen/Rollennamen das Attribut organame verwenden. Die Mappings sehen dann wie folgt aus:

```
<CN>
      <vipattr>cn</vipattr>
      <ldapattr>fullname</ldapattr>
</CN>
<LDAP_USER_NAME>
      <vipattr>userclass.name</vipattr>
      <ldapattr>fullname</ldapattr>
      <ldapread>false</ldapread>
</LDAP_USER_NAME>
<LDAP_GROUP_NAME>
      <vipattr>groupclass.name</vipattr>
      <ldapattr>organame</ldapattr>
      <ldapread>false</ldapread>
</LDAP_GROUP_NAME>
<LDAP_ROLE_NAME>
      <vipattr>roleclass.name</vipattr>
      <ldapattr>organame</ldapattr>
      <ldapread>false</ldapread>
</LDAP_ROLE_NAME>
<READ_PRINCIPAL_NAME>
      <vipattr>principal.name</vipattr>
      <ldapattr>organame</ldapattr>
      <ldapread>true</ldapread>
```

```
      <ldapwrite>false</ldapwrite>
</READ_PRINCIPAL_NAME>
```

LDAP-Abfragen beschleunigen

Zur Beschleunigung von LDAP-Abfragen durch Livelink WCM Server können Sie verschiedene Konfigurationsmöglichkeiten nutzen. Dazu gehören Indexierungsfunktionen im LDAP-Server und inverse Attribute.

Index des LDAP-Servers nutzen

Bei einigen LDAP-Verzeichnisdiensten können Attribute in einen Index aufgenommen werden. Auf diese Weise werden Suchabfragen nach Objekten mit diesem Attribut beschleunigt. Folgende WCM-Attribute sollten indexiert werden:

- `vipFuncarea`, `vipWebsite` und `vipSubstitute` (WCM-Attribute, in denen Zuordnungen gespeichert werden)
- `uid` bzw. `cn` (WCM-Attribut, aus dem die Benutzerkennungen ausgelesen werden)
- `member` bzw. `uniquemember` (WCM-Attribut, in dem die Benutzer einer Gruppe oder Rolle gespeichert sind)
- `objectclass`
- In Microsoft Active Directory sollte auch `vipType` indexiert werden.

Inverse LDAP-Attribute nutzen

Werden im LDAP-Verzeichnisdienst sehr viele Gruppen und Benutzer verwaltet, kann das Abfragen bestimmter Benutzereinstellungen wie z.B. der Gruppenzugehörigkeit sehr lange dauern. Um solche Abfragen zu beschleunigen, kann Livelink WCM Server so genannte *inverse LDAP-Attribute* nutzen.

Inverse Attribute speichern umgekehrte Zuordnungen – so können im LDAP-Attribut `memberof` der Klasse `vipUser` z.B. die Gruppen bzw. Rollen gespeichert werden, zu denen der Benutzer gehört. Ein weiteres inverses Attribut, das Livelink WCM Server nutzen kann, ist `substituteof` zur Speicherung von Stellvertreterzuordnungen.

Wenn diese Attribute korrekt gemappt und gesetzt wurden und die Einstellungen bzw. Zuordnungen eines Benutzers, z.B. über den Admin-Client, abgefragt werden, werden nicht alle Gruppen durchsucht, um festzustellen, ob der gewählte Benutzer dazugehört. Stattdessen wird nur das Attribut `memberof` ausgewertet. Analog erfolgt der Zugriff auf Stellvertreter.

Hinweise:

Livelink WCM Server kann diese Attribute nutzen, um Abfragen beschleunigt durchzuführen. Die Pflege dieser Attribute muss jedoch außerhalb des WCM-Systems erfolgen.

Sie sollten diese Attribute nur für Livelink WCM Server nutzbar machen, wenn in Ihrem LDAP-Verzeichnisdienst eine sehr große Anzahl an Gruppen und Rollen verwaltet wird und Performance-Probleme beim Abfragen von Benutzerdaten auftreten.

Wenn Sie inverse LDAP-Attribute nutzen möchten, fügen Sie der Objektklasse `vipUser` die folgenden Attribute hinzu:

Tabelle 6 – Inverse LDAP-Attribute für die Klasse `vipUser`

WCM-Attribut	Datentyp (Syntax)	Single-Value	Mapping WCM-Attribut → LDAP-Attribut
`vipMemberOf`	DN		`vipMemberOf` → `memberof`
`vipSubstitueOf`	DN		`vipSubstituteOf` → `substituteof`

Diese Attribute müssen in der Datei **ldapmapping.xml** im Verzeichnis **{WCM-Installationsverzeichnis}\config** auf die Attribute des verwendeten LDAP-Verzeichnisdienstes gemappt werden.

Beispiel (Active Directory):

```
...
<VIP_MEMBEROF>
      <vipattr>vipMemberOf</vipattr>
      <ldapattr>memberof</ldapattr>
</VIP_MEMBEROF>
<VIP_SUBSTITUTEOF>
      <vipattr>vipSubstituteOf</vipattr>
      <ldapattr>substituteof</ldapattr>
</VIP_SUBSTITUTEOF>
...
```

Separates Verzeichnis für WCM-Benutzer anlegen

Werden in dem LDAP-Verzeichnisdienst viele Benutzer mit zahlreichen Attributen verwaltet, von denen nur ein Teil auf das WCM-System zugreifen soll und bei denen auch nur ein Teil der Attribute WCM-relevant sind, empfehlen wir, diese Benutzer mit den WCM-relevanten Attributen in ein separates Verzeichnis auszulagern (z. B. über den Replikationsmechanismus des LDAP-Verzeichnisdienstes). Auf diese Weise beschleunigen Sie den Zugriff auf das WCM-System.

3.3 LDAP-Bindeprofil und WCM-Administrator einrichten

Der Zugriff von Livelink WCM Server auf den LDAP-Verzeichnisdienst erfolgt über das so genannte LDAP-Bindeprofil, d. h. eine Verbindung mit lesendem und schreibendem Zugriff auf die WCM-spezifischen Objektklassen bzw. Attribute.

Für diese Verbindung nutzt Livelink WCM Server das Verfahren “Simple Authentication”, d.h., die jeweilige Authentifizierung wird mittels eines in Klartext übertragenen Kennworts vorgenommen. Um die Sicherheit zu erhöhen, kann die Verbindung zum LDAP-Verzeichnisdienst über SSL (Secure Socket Layer) erfolgen (siehe Abschnitt 3.5 “SSL-Verbindung zum LDAP-Server verwenden” auf Seite 64).

Bei der Installation von Livelink WCM Server muss zusätzlich ein Benutzer als WCM-Administrator angegeben werden. Dieser Benutzer muss daher zum Zeitpunkt der WCM-Installation bereits im LDAP-Verzeichnisdienst eingerichtet sein.

LDAP-Bindeprofil einrichten

Der Zugriff von Livelink WCM Server auf den LDAP-Verzeichnisdienst erfolgt über eine personalisierte Verbindung. Diese Verbindung setzt die Existenz eines Bindeprofils in LDAP voraus, über das alle Lese- und Schreibzugriffe von Livelink WCM Server abgewickelt werden. Bei der Installation von Livelink WCM Server wird das Bindeprofil mit Kennwort angegeben (siehe Abschnitt “Parameter des LDAP-Verzeichnisdienstes einstellen” auf Seite 88).

Sie können für dieses Bindeprofil die Angaben des bereits vorhandenen LDAP-Administrators verwenden. Möchten Sie dies nicht tun, muss das Bindeprofil in LDAP neu angelegt werden. Bitte beachten Sie dabei Folgendes:

- Aus Sicherheitsgründen sollte der Benutzer außerhalb des von Livelink WCM Server zugreifbaren Namensraums liegen. Auf diese Weise wird verhindert, dass über den Admin-Client auf die Eigenschaften des Bindeprofils zugegriffen werden kann.
- Der Benutzer muss lesenden und schreibenden Zugriff auf die vom WCM-System verwendeten Attribute ab dem angegebenen Suchknoten haben.

WCM-Administrator einrichten

Während der Installation richten Sie einen Benutzer als WCM-Administrator ein (siehe Abschnitt “WCM-Administrator einrichten” auf Seite 93). Dieser Benutzer muss vor der Installation bereits in LDAP existieren und mit den folgenden WCM-Attributen ausgestattet sein:

- `vipAccess`, Wert = `true` (d.h. aktiv)
- `cn`
- `mail`
- `uid`
- `vipLanguage`, Wert = `de_DE` oder `en_US` (locale)
- `userPassword`
- `initPassword`, Wert = `false`
- `trustedLogin`, Wert = `false`
- Für Microsoft Active Directory: `vipType`, Wert = `vipUser`
- Für Novell eDirectory, Sun ONE Directory Server und OpenLDAP: Im Attribut `objectclass` muss der Wert `vipUser` hinzugefügt werden.

Für diesen Benutzer sind keine spezifischen Schreibrechte erforderlich, da er im Unterschied zum LDAP-Bindeprofil ein “normaler” WCM-Benutzer ist. Der WCM-Administrator muss in dem Namensraum angelegt werden, auf den Livelink WCM Server zugreift. Nur dann kann sich der Administrator am WCM-System anmelden.

3.4 Hinweise zur Verwendung mehrerer LDAP-Server

Mit Livelink WCM Server ist es möglich, auf mehrere LDAP-Server zuzugreifen. Dies kann erforderlich sein, wenn in einem Unternehmen verschiedene LDAP-Server zur Verwaltung von Benutzerinformationen oder Fallback-LDAP-Server zur Erhöhung der Ausfallsicherheit eingesetzt werden. Die zusätzlichen LDAP-Server werden mithilfe von weiteren LDAP-Pools in das WCM-System eingebunden. Im Admin-Client ist einstellbar, in welcher Reihenfolge auf die LDAP-Server zugegriffen werden soll. Ist ein LDAP-Server nicht erreichbar, wird er für eine gewisse Zeitspanne ignoriert.

Hinweis: Bitte beachten Sie, dass beim Einsatz mehrerer LDAP-Server – für verschiedene Administrationsserver bzw. bei Verwendung von Fallback-Servern – die Daten zwischen den LDAP-Servern zeitnah repliziert werden müssen.

Außerdem ist es möglich, dass mehrere WCM-Systeme die Benutzerinformationen desselben LDAP-Servers benutzen. Hinweise dazu finden Sie im Abschnitt “Benutzerinformationen in verschiedenen WCM-Systemen verwenden” auf Seite 62.

Fallback-LDAP-Server verwenden

Um die Ausfallsicherheit zu erhöhen, können Fallback-LDAP-Server eingesetzt werden, die beim Ausfall des primären LDAP-Servers dessen Aufgaben übernehmen. Damit diese Fallback-Server auch vom WCM-System angesprochen werden können, müssen Sie nach der Installation über den Admin-Client einen LDAP-Pool mit den Angaben des Fallback-LDAP-Servers einrichten und diesen Pool dem Admin-Server zuordnen. Informationen zum Anlegen und Zuordnen neuer Pools erhalten Sie im Livelink WCM Server-Administratorhandbuch.

Hinweise:

Bei der Installation von Livelink WCM Server wird der primäre LDAP-Server angegeben (siehe Abschnitt “Parameter des LDAP-Verzeichnisdienstes einstellen” auf Seite 88).

Das WCM-System unterscheidet beim Zugriff nicht, ob es sich um einen primären LDAP-Server, einen alternativen LDAP-Server oder ein Fallback-System handelt. Beachten Sie dies bei der Konfiguration des Fallback-LDAP-Servers.

Benutzerinformationen aus mehreren LDAP-Servern verwenden

Nutzen Sie in Ihrem Unternehmen mehrere LDAP-Server zur Verwaltung von Benutzerinformationen, kann Livelink WCM Server auch auf unterschiedliche LDAP-Server zugreifen. So ist es z.B. möglich, sowohl der Gruppe “Marketing” vom LDAP-Server A als auch der Gruppe “Sales” vom LDAP-Server B Zugriff auf Ihr WCM-System zu ermöglichen.

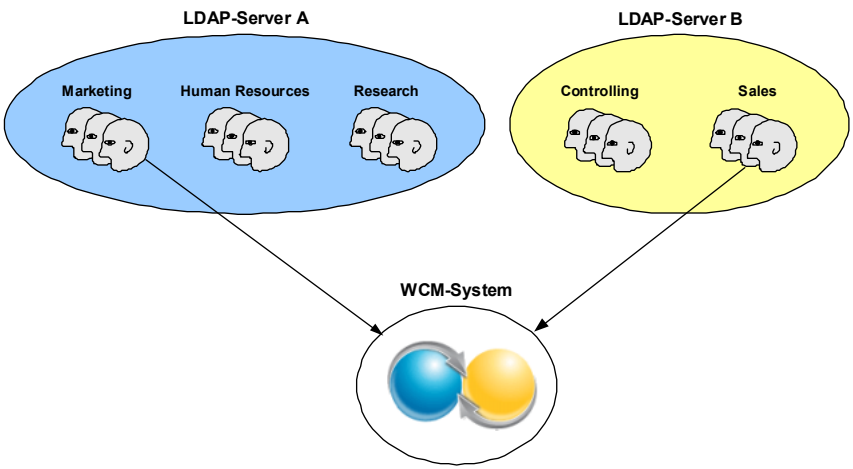


Abb. 2 – Verwendung mehrerer LDAP-Server

Bei der Installation von Livelink WCM Server wird zunächst der LDAP-Server angegeben, auf dem der zukünftige WCM-Administrator verwaltet wird, z.B. LDAP-Server A (siehe Abschnitt “Parameter des LDAP-Verzeichnisdienstes einstellen” auf Seite 88 und “WCM-Administrator einrichten” auf Seite 93). Nach der Installation können Sie im Admin-Client die Benutzer der Gruppe “Marketing” von LDAP-Server A mit den WCM-Attributen ausstatten.

Um auch den Benutzern der Gruppe “Sales” von LDAP-Server B den Zugriff auf das WCM-System zu ermöglichen, legen Sie über den Admin-Client einen neuen LDAP-Pool mit den Verbindungsdaten dieses Servers an und ordnen den Pool dem Admin-Server zu. Nun können Sie auch die Benutzer der Gruppe “Sales” mit den WCM-Attributen ausstatten und ihnen so den Zugriff auf das WCM-System ermöglichen.

Hinweise

- Informationen darüber, wie Sie mithilfe des Admin-Clients LDAP-Benutzer mit den WCM-Attributen ausstatten, erhalten Sie im Livelink WCM Server-Administratorhandbuch (Kapitel “Benutzerverwaltung”).
- Die LDAP-Position der Principals (Benutzer, Gruppen und Rollen) ist im WCM-System ohne Bedeutung. Die Principals werden in einer flachen Liste im Admin-Client dargestellt.
- Die Benutzerkennungen müssen für alle eingestellten LDAP-Zweige eindeutig sein, da die Benutzer im WCM-System nur anhand ihrer Kennung, nicht anhand von Gruppen- oder Rollenzugehörigkeiten oder ihrer Position im LDAP-Baum unterschieden werden.

  Auch die Gruppen- und Rollennamen müssen im WCM-System eindeutig sein.

- Beim Neuanlegen von Benutzern, Gruppen und Rollen muss eine eindeutige Zuordnung des neuen Principals zu einem LDAP-Server erfolgen, wenn unterschiedliche Suchknoten verwendet werden. Geben Sie dazu beim Anlegen des Principals die korrekte LDAP-Position an.

Benutzerinformationen in verschiedenen WCM-Systemen verwenden

Es ist auch möglich, Benutzerinformationen aus einem LDAP-Verzeichnisdienst für mehrere installierte WCM-Systeme zu verwenden. Die folgende Grafik veranschaulicht ein solches Szenario. Die Benutzer der Gruppe “Marketing” haben Zugriff auf zwei WCM-Systeme, während die Gruppe “Sales” nur Zugriff auf das WCM-System B hat.

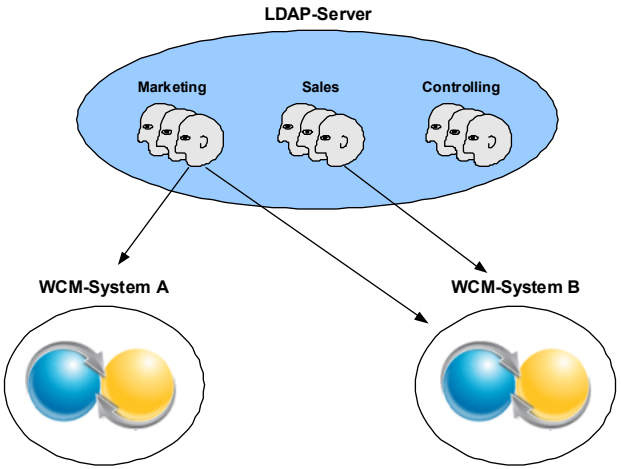


Abb. 3 – Nutzung eines LDAP-Servers für mehrere WCM-Systeme

Zur Konfiguration einer solchen Anbindung haben Sie zwei Möglichkeiten:

- Für beide WCM-Systeme werden dieselben LDAP-Objektklassen und Attribute verwendet.

  Damit haben die Benutzer der Gruppe “Marketing” in beiden WCM-Systemen die gleichen Einstellungen. Wenn Sie einem Benutzer dieser Gruppe den Zugriff auf das WCM-System A sperren, kann er auch nicht mehr auf das WCM-System B zugreifen, da das entsprechende Attribut (`vipAccess`) nur einmal vorhanden ist.

- Für die beiden WCM-Systeme werden unterschiedliche LDAP-Objektklassen und Attribute verwendet. Dies gibt Ihnen die Möglichkeit, die Einstellungen der Benutzer für die WCM-Systeme separat zu steuern.

  In unserem Beispiel werden die Benutzer der Gruppe “Marketing” mit den Objektklassen beider WCM-Systeme ausgestattet. Attribute, die für die WCM-Systeme separat gesteuert werden sollen, werden pro WCM-System angelegt. So werden beispielsweise zwei Attribute für den Zugriff auf das WCM-System angelegt: `vipAccessA` und `vipAccessB`.

  Die Zuordnung der verschiedenen Attribute zum WCM-System erfolgt über das Mapping der WCM- und LDAP-Attribute (siehe Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45).

  Die folgende Tabelle veranschaulicht eine Beispielkonfiguration:

Tabelle 7 – Beispielkonfiguration für separate LDAP-Objektklassen und -attribute

	WCM-System A	WCM-System B	LDAP-Principal
Objektklasse	`vipUserA`	`vipUserB`	`vipUserA` und `vipUserB`
WCM-Zugriff (separate Steuerung)	Mapping auf das Attribut `vipaccessA`	Mapping auf das Attribut `vipaccessB`	`vipaccessA =true` `vipaccessB =false`
Vertraute Anmeldung (gleich für beide WCM-Systeme)	Mapping auf das Attribut `trustedLogin`	Mapping auf das Attribut `trustedLogin`	`trustedlogin =false`

3.5 SSL-Verbindung zum LDAP-Server verwenden

Um die Übertragung von LDAP-Passwörtern im Klartext über das Netzwerk zu verhindern und damit die Sicherheit zu erhöhen, kann für die Verbindung des WCM-Systems mit dem LDAP-Verzeichnisdienst das Verfahren SSL (Secure Socket Layer) verwendet werden. Zu diesem Zweck muss der verwendete LDAP-Server einen SSL-Port bieten, und das Serverzertifikat muss als Datei vorliegen. Für weitere Informationen wenden Sie sich bitte an den Hersteller des verwendeten LDAP-Verzeichnisdienstes.

Die Verwendung von SSL kann bei der Installation von Livelink WCM Server aktiviert werden (siehe Abschnitt “Parameter des LDAP-Verzeichnisdienstes einstellen” auf Seite 88). Sie können SSL jedoch auch nachträglich in den Einstellungen des entsprechenden

LDAP-Pools aktivieren (siehe Livelink WCM Server-Administratorhandbuch).

Damit SSL verwendet werden kann, muss zuvor das Serverzertifikat dem WCM-Truststore hinzugefügt werden. Dies erfolgt mithilfe des so genannten Keytools, das über die Konsole aufgerufen wird. Das Keytool befindet sich im Verzeichnis **{Java SDK-Verzeichnis}\bin**.

SSL bei der Installation nutzen

Bevor Sie die Installation des WCM-Systems starten, sind folgende Arbeiten erforderlich:

- Installation erfolgt von der Festplatte: Wenn Sie die Dateien von der WCM-CD auf Ihre Festplatte kopieren, gehen Sie vor wie im folgenden Abschnitt beschrieben. Der Platzhalter "{WCM-Installationsverzeichnis}" steht in diesem Fall für das Verzeichnis auf Ihrer Festplatte, in dem die Installationsdateien gespeichert sind.
- Installation erfolgt von der WCM-CD: Wenn Sie die Installation direkt von der Installations-CD vornehmen möchten, gehen Sie folgendermaßen vor:

  1. Kopieren Sie die Datei **gauss_vip80.trust** aus dem Verzeichnis **\keys** von der WCM-CD in ein temporäres Verzeichnis.
  2. Führen Sie die Schritte aus, die im folgenden Abschnitt beschrieben sind.
  3. Passen Sie das Installationsskript **install.bat** bzw. **.sh** an, indem Sie den Ausdruck

```
java -Xmx64m de.gauss.vip.installation.Installation
```

     ersetzen durch

```
java -Xmx64m -Djavax.net.ssl.truststore={Speicherort der Datei
   gauss_vip80.trust} de.gauss.vip.installation.Installation
```

LDAP-Serverzertifikat dem WCM-Truststore hinzufügen

So fügen Sie das LDAP-Serverzertifikat dem WCM-Truststore hinzu:

1. Kopieren Sie die Datei mit dem Serverzertifikat für den LDAP-Server in das Verzeichnis **{WCM-Installationsverzeichnis}\keys**.
2. Öffnen Sie die Eingabeaufforderung.
3. Wechseln Sie in das WCM-Installationsverzeichnis und anschließend in das Unterverzeichnis **\keys**.
4. Überprüfen Sie, ob das kopierte Serverzertifikat vom Keytool verwendet werden kann. Geben Sie dazu folgenden Befehl ein:

```
keytool -printcert -file {Dateiname des Serverzertifikats}
```

5. Überprüfen Sie die Ausgaben des Keytools. Das Tool gibt u.a. die “Fingerprints” des Zertifikats auf der Konsole aus.
6. Wenn die Überprüfung erfolgreich war, starten Sie das Hinzufügen des Serverzertifikats zum WCM-Truststore z.B. mit dem folgenden Aufruf:

```
keytool -import -alias {Alias} -v -file {Dateiname des Server-
   zertifikats} -keypass {Passwort} -keystore gauss_vip80.trust
   -storepass changeit
```

   Die folgende Tabelle erläutert die Parameter des Aufrufs, die entsprechend Ihrem System geändert werden müssen. Die Werte, die Sie anpassen müssen, sind in geschweifte Klammern gesetzt, z.B. {Passwort}.

Tabelle 8 – Parameter für Keytool

Parameter	Erläuterung
`-alias {Alias}`	Name, unter dem das Serverzertifikat im WCM-Truststore abgespeichert wird
`-v`	Parameter für die Ausführlichkeit der Ausgaben des Keytools auf der Konsole `-v` bedeutet ausführliche Ausgaben (verbose).
`-file {Serverzertifikat}`	Name der Datei mit dem Serverzertifikat
`-keypass {Passwort}`	Passwort für die Datei mit dem Serverzertifikat
`-keystore {WCM-Truststore}`	Name des WCM-Truststores, das unter **{WCM-Installationsverzeichnis}\keys** gespeichert ist Standard = `gauss_vip80.trust`
`-storepass {Passwort}`	Passwort für den WCM-Truststore Standard = `changeit`

7. Überprüfen Sie mit dem folgenden Befehl, ob das Serverzertifikat erfolgreich installiert wurde.

```
keytool -list -v -keystore gauss_vip80.trust -storepass changeit
```

Die Ausgabe für das Serverzertifikat muss mit den Angaben übereinstimmen, die bei der Überprüfung unter Punkt 5 ausgegeben wurden.

Beispiel

```
Keystore type: jks
Keystore provider: SUN

Your keystore contains 12 entries:

..

Alias name: {Alias}
Creation date: Tue Mar 28 12:52:01 GMT+01:00 2002
Entry type: trustedCertEntry

Owner: CN=Admin, OU=Development, O=Company, C=DE
Issuer: CN=Thawte Test CA Root, OU=TEST TEST TEST, O=Thawte
   Certification, ST=FOR TESTING PURPOSES ONLY, C=ZA
Serial number: 268114
Valid from: Tue Mar 05 15:30:19 GMT+01:00 2002 until: Tue Mar 26
   15:30:19 GMT+01:00 2002
Certificate fingerprints:
       MD5:  5C:82:D7:01:AF:F9:5C:25:E7:F5:EE:D0:AE:DC:3D:ED
       SHA1: 36:5A:82:3D:B9:7B:32:2A:38:57:83:02:DD:F5:36:82:C6:
             BC:13:BA
```

Das Serverzertifikat aus unserem Beispiel wurde erfolgreich dem WCM-Truststore hinzugefügt.

KAPITEL 4

Installation von Livelink WCM Server

Mithilfe des Installationsprogramms von Livelink WCM Server können Sie verschiedene Aufgaben realisieren. Die folgende Abbildung liefert Ihnen eine Übersicht über die verschiedenen Installationsmöglichkeiten.

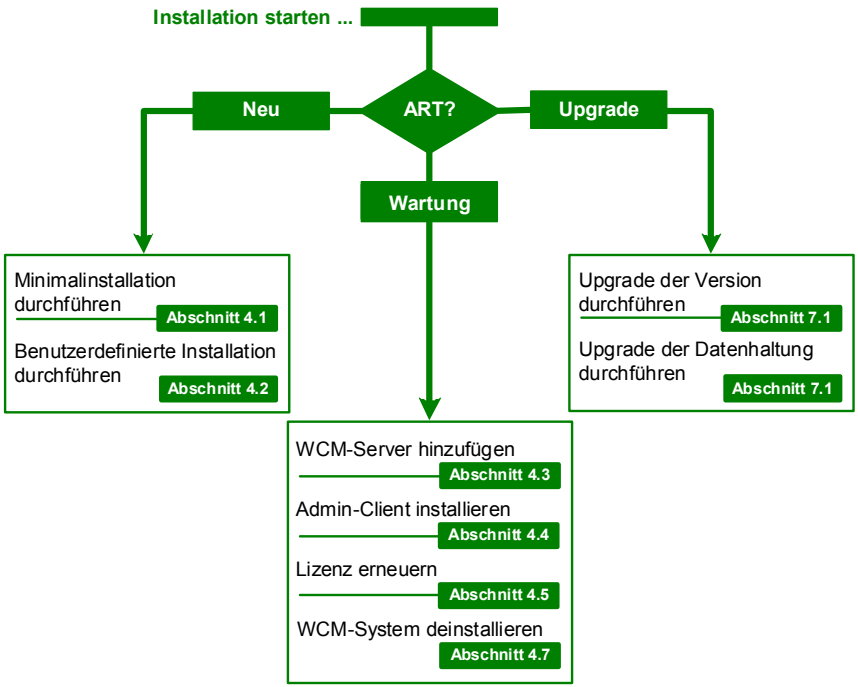


Abb. 4 – Installationsmöglichkeiten im Überblick

Neben der Installation über die grafische Oberfläche ist auch eine Konsoleninstallation möglich (siehe Abschnitt 4.8 “Installation und Deinstallation über die Konsole steuern” ab Seite 135).

Außerdem erhalten Sie in diesem Kapitel Informationen zum Starten und Stoppen der Server (siehe Abschnitt 4.9 “Server starten und stoppen” auf Seite 162). In Abschnitt 4.10 “Protokoll- und Fehlerdateien” auf Seite 174 finden Sie Angaben zu den Protokollen, die bei der Installation und beim Starten bzw. Stoppen der Server angelegt werden.

4.1 Neues WCM-System installieren (Minimalsystem)

Die Installation des WCM-Systems erfolgt mithilfe des WCM-eigenen Installationsprogramms. Während des Installationsvorgangs werden Sie durch einen Assistenten unterstützt, über den alle erforderlichen Angaben gemacht werden.

In diesem Abschnitt wird die Installation eines Minimalsystems beschrieben. Informationen zur Architektur von WCM-Systemen erhalten Sie im Livelink WCM Server-Administratorhandbuch (Kapitel “Konzepte”).

Hinweise zur Installation

- Für die Installation sind gültige Lizenzen aller entsprechenden WCM-Komponenten erforderlich.
- Wenn Sie die Server unter Windows als Dienst einrichten möchten, benötigen Sie lokale Administratorrechte.
- Unter UNIX sollten die Server grundsätzlich nicht mit der uid “0” bzw. “root” installiert und betrieben werden.
- Unter UNIX muss vor der Installation der Server ein Benutzer für die Server eingerichtet werden (z.B. “wcmuser”).

- Um mit dem Content-Client, dem Content-Client (Classic) und InSite Editing arbeiten zu können, ist mindestens ein Content-Server erforderlich, der im Kontext der JSP-Engine bzw. als Webanwendung im Application-Server läuft.
- Alle notwendigen Angaben zum WCM-System werden während der Installation gemacht. In bestimmten Fällen ist es notwendig, bereits vor der Installation einige Einstellungen in der Datei **defaults.xml** vorzunehmen. Diese Datei befindet sich im Verzeichnis **\installation** auf der WCM-CD und enthält sämtliche Standardeinstellungen für die Installation.

  Um z.B. für das Mapping von LDAP-Attributen in dieser Datei Änderungen vorzunehmen, kopieren Sie sie auf ein lokales Laufwerk. Beim Aufruf der Installation kann dann der Pfad zur Datei **defaults.xml** als Parameter übergeben werden.
- Sie können bereits bei der Installation von Livelink WCM Server für die Verbindung des WCM-Systems mit dem LDAP-Verzeichnisdienst das Verfahren SSL (Secure Socket Layer) verwenden. Hierzu sind vor der Installation bestimmte Arbeiten auszuführen (siehe Abschnitt “SSL bei der Installation nutzen” auf Seite 65).

Installation starten

Das Installationsprogramm wird unter Windows und UNIX unterschiedlich gestartet:

- **Windows:** Öffnen Sie die MS-DOS-Eingabeaufforderung, wechseln Sie auf das CD-ROM-Laufwerk, und rufen Sie das Installationsprogramm mit dem Pfad auf Ihr Java 2 SDK-Verzeichnis als Parameter auf. Der Pfad zur Datei **defaults.xml** (inklusive Dateiname) muss nur angegeben werden, wenn statt der Standarddatei auf der WCM-CD eine lokal gespeicherte Datei verwendet werden soll.

```
install.bat {SDK-Installationsverzeichnis}\bin
   {Pfad zur Datei defaults.xml}
```

- **UNIX:** Auf der WCM-CD wird ein JAR-Archiv mitgeliefert. Übertragen Sie dieses Archiv auf Ihren Server, und entpacken Sie es in ein temporäres Verzeichnis. Wechseln Sie in dieses Verzeichnis und rufen Sie von dort aus das Installationsskript mit dem Pfad auf Ihr Java 2 SDK-Verzeichnis und dem Pfad zur Datei **defaults.xml** (inklusive Dateiname) als Parameter auf.

  ```
  sh ./install.sh [-jdk {SDK-Installationsverzeichnis}/bin]
     [-defaults {Pfad zur Datei defaults.xml}]
  ```

  Wenn Sie das Installationsskript ohne Parameter aufrufen, werden Sie anschließend aufgefordert, den Pfad auf Ihr Java 2 SDK-Verzeichnis (**{SDK-Installationsverzeichnis}/bin/**) und die Datei **defaults.xml** einzugeben.

Nach erfolgter Eingabe wird die grafische Oberfläche der Installation gestartet.

Beim Installationsvorgang werden Sie durch einen Assistenten unterstützt. Folgen Sie den Anweisungen auf dem Bildschirm. Die folgende Beschreibung enthält zusätzliche Informationen, die über die Anweisungen des Assistenten hinausgehen.

Installationsverzeichnis auswählen

Wenn Sie ein neues WCM-System installieren, geben Sie ein lokales Verzeichnis an, in dem sich noch keine WCM-Komponenten befinden.

Wenn Sie bereits ein WCM-System installiert haben und neue Server hinzufügen möchten, gibt es zwei Möglichkeiten:

- Soll der neue Server in dem gleichen Verzeichnis wie das bestehende WCM-System installiert werden, dann geben Sie das WCM-Installationsverzeichnis an.
- Soll der neue Server in ein anderes Verzeichnis installiert werden, geben Sie dieses an.

Hinweis: Beachten Sie bei der Installation unter UNIX, dass das Installationsverzeichnis kein symbolischer Link sein darf.

Bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Weiter*.

Typ der Installation auswählen

In diesem Dialog legen Sie fest, was Sie installieren möchten.

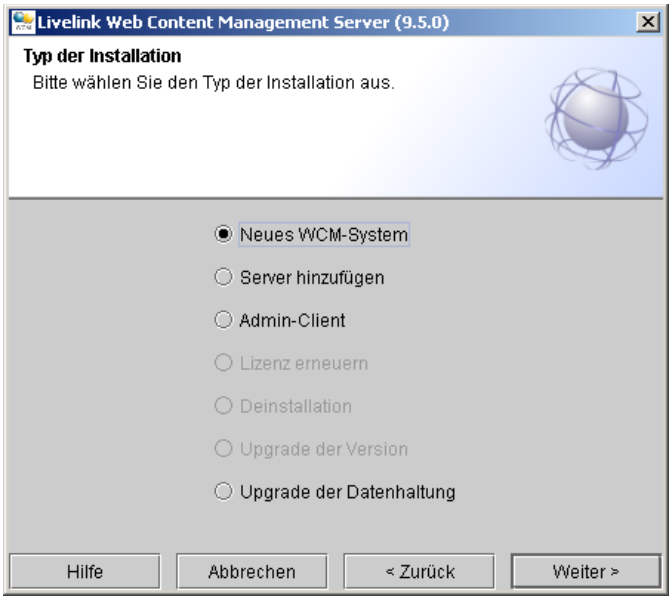


Abb. 5 – Optionen beim Installationsvorgang

Hinweis: Wenn Sie bei der Festlegung des Installationsverzeichnisses ein Verzeichnis ausgewählt haben, in dem bereits ein WCM-System installiert wurde, ist die Option *Neues WCM-System* automatisch deaktiviert.

- *Neues WCM-System:* Aktivieren Sie dieses Optionsfeld, um ein neues WCM-System einzurichten.
- *Server hinzufügen*, siehe Abschnitt 4.3 “Neue Server hinzufügen” auf Seite 118
- *Admin-Client*, siehe Abschnitt 4.4 “Admin-Client installieren” auf Seite 122
- *Lizenz erneuern*, siehe Abschnitt 4.5 “Lizenz erneuern” auf Seite 124

- *Deinstallation*, siehe Abschnitt 4.7 “WCM-System deinstallieren” auf Seite 130
- *Upgrade der Version*, siehe Abschnitt “Upgrade der Version durchführen” auf Seite 228
- *Upgrade der Datenhaltung*, siehe Abschnitt “Upgrade der Datenhaltung durchführen” auf Seite 231

Aktivieren Sie das gewünschte Optionsfeld, und klicken Sie auf die Schaltfläche *Weiter*.

Optionen für die Lizenzverwaltung festlegen

In diesem Dialog legen Sie die Optionen für die Lizenzverwaltung fest.

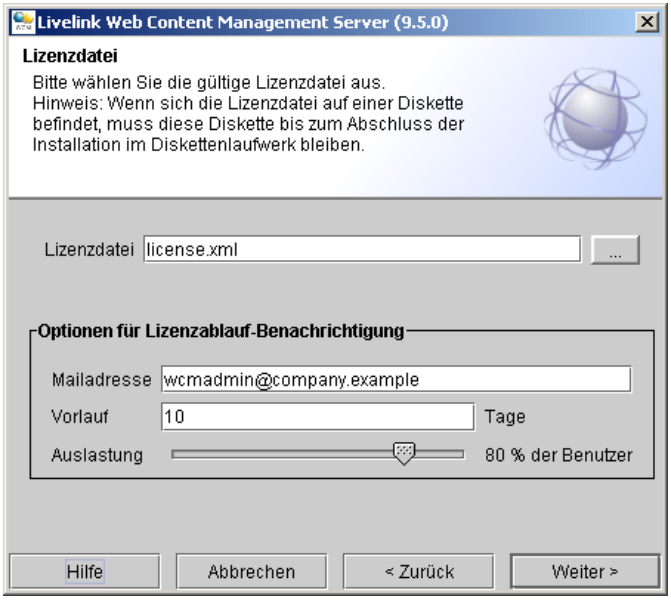


Abb. 6 – Optionen für die Lizenzverwaltung festlegen

- *Lizenzdatei:* Wählen Sie mithilfe der Schaltfläche ... den Pfad zur mitgelieferten Lizenzdatei **license.xml** aus.
- *Mailadresse:* E-Mail-Adresse des Verantwortlichen, der bei Ablauf oder Überschreitung der WCM-Lizenzen per E-Mail benachrichtigt werden soll
- *Vorlauf:* Anzahl der Tage vor Ablauf der Lizenzen. Ist dieser Zeitpunkt erreicht, wird automatisch eine entsprechende Nachricht an die angegebene E-Mail-Adresse gesendet.
- *Auslastung ... % der Benutzer:* Prozentsatz der ausgelasteten Lizenzen für aktive Benutzer. Wird diese Prozentzahl überschritten, wird automatisch eine entsprechende Nachricht an die angegebene E-Mail-Adresse gesendet.

> **Hinweise:**
>
> Diese Einstellungen können Sie nach der Installation im Admin-Client über *Konfiguration* → *Dienstprogramme* → *Lizenzablaufbenachrichtigung* ändern.
>
> Den Zustand Ihrer WCM-Lizenzen können Sie jederzeit über *Systemverwaltung* → *Lizenzen* überprüfen.

Bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Weiter*.

Parameter des neuen Administrationsservers einstellen

In diesem Dialog legen Sie die Parameter des neuen Administrationsservers fest.

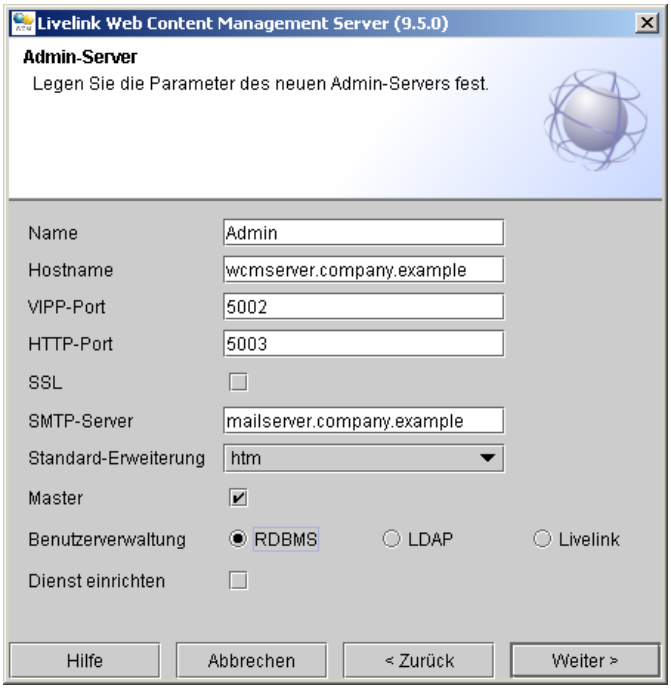


Abb. 7 – Parameter des Administrationsservers

- *Name:* Name des Servers. Dieser Name ist frei wählbar, muss jedoch innerhalb des WCM-Systems eindeutig sein. Folgende Zeichen sind erlaubt:
  - a–z, A–Z, 0–9 (ASCII 7 Bit)
  - . (Punkt), _ (Unterstrich) und - (Bindestrich)

- *Hostname:* voll qualifizierter Hostname des Rechners, auf dem dieser Server installiert werden soll

  Standardmäßig wird versucht, den Namen des aktuellen Rechners zu ermitteln. Wenn das nicht möglich ist, wird der Standardeintrag “localhost” eingetragen. Dieser Eintrag sollte jedoch geändert werden, da er bei verteilten Systemen zu Problemen führt.

- *VIPP-Port* und *HTTP-Port:* Port-Nummern des Servers für die Verbindung über das Protokoll VIPP bzw. HTTP. Das Installationsprogramm legt einen Pool für die Verbindungen zu diesem Server an, der den Namen des entsprechenden Servers erhält.

  Hinweise:

  Achten Sie darauf, dass die angegebenen Port-Nummern nicht von anderen Anwendungen verwendet werden. Sind zwischen den einzelnen Servern oder zwischen Client und Server Firewalls vorhanden, sind die entsprechenden Port-Adressen freizuschalten.

  Nach der Installation können Sie über den Admin-Client weitere Parameter für die Kommunikation über das entsprechende Protokoll festlegen (Ansicht *Konfiguration* → *Pools* → *WCM* → *{Poolname}* → Registerkarte *WCM-Verbindung*).

- *SSL:* Durch Aktivieren des Kontrollkästchens *SSL* können Sie festlegen, dass die Kommunikation zwischen den Servern über gesicherte Verbindungen (Secure Socket Layer) erfolgt.

- *SMTP-Server:* voll qualifizierter Hostname des Rechners, auf dem der SMTP-Server installiert ist. Die Adresse des SMTP-Servers können Sie nach der Installation im Admin-Client in den Server-Einstellungen ändern (Register *Verschiedenes*).

- *Standard-Erweiterung:* Wählen Sie hier die Standard-Dateinamenerweiterung für generierte Seiten aus. Die generierten Seiten sind die Dateien, die von den Deploymentsystemen aus den WCM-Objekten erzeugt und im lokalen Dateisystem der Server abgelegt werden.

- *Master:* Aktivieren Sie dieses Kontrollkästchen, um den Administrationsserver als Master-Admin-Server einzurichten. Wenn Sie einen Proxy-Admin-Server installieren möchten, deaktivieren Sie das Kontrollkästchen.
- *Benutzerverwaltung:* Wählen Sie hier, ob der Administrationsserver die Benutzerdaten in einem relationalen Datenbank-Managementsystem, in einem LDAP-Verzeichnisdienst oder in Livelink speichern soll.

  Hinweis: Wenn die Benutzerdaten des Livelink-Systems durch Synchronisation aus einem LDAP-Verzeichnisdienst gelesen werden, aktivieren Sie hier das Optionsfeld *LDAP*.

- *Dienst einrichten:* Mit dieser Option legen Sie unter Windows fest, ob der Administrationsserver als Dienst (zum automatischen Starten und Beenden des Servers) eingerichtet wird.

  Hinweis: Mithilfe der Skripte **install_{Servername}.bat** im Verzeichnis **{WCM-Installationsverzeichnis}\installation \service** können Sie auch nach der Installation Dienste für die Server einrichten.

Bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Weiter*.

Parameter des RDBMS einstellen

Wenn Sie bei der Einrichtung des Admin-Servers unter *Benutzerverwaltung* das Optionsfeld *RDBMS* aktiviert haben, sind im nächsten Dialog die Parameter für die Verbindung zur Datenbank festzulegen.

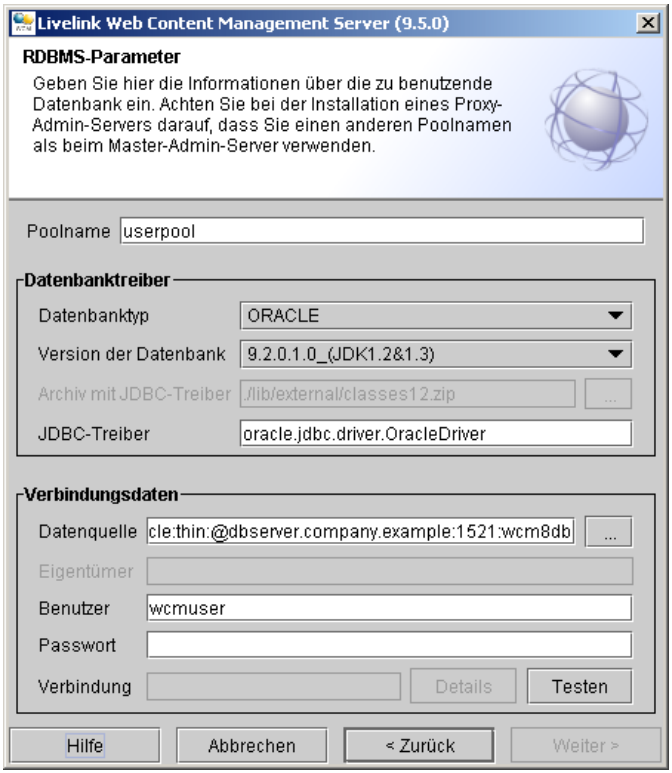


Abb. 8 – Parameter der zu benutzenden Datenbank

Poolname: Name des JDBC-Pools, der für die Verbindungen zum RDBMS angelegt wird

> **Achtung!** Stellen Sie bei der Installation eines Proxy-Admin-Servers sicher, dass ein anderer Name als für den Pool des Master-Admin-Servers verwendet wird.

Bereich *Datenbanktreiber*

- *Datenbanktyp:* Typ des verwendeten RDBMS. Sie können wählen zwischen
  - ORACLE
  - MS SQL Server 2000
- *Version der Datenbank* (nur für Oracle): Version des verwendeten RDBMS Oracle. Sollte die von Ihnen verwendete Version in der Auswahlliste nicht enthalten sein, wählen Sie den Eintrag “Manuelle Auswahl des Archivs”.
- *Archiv mit JDBC-Treiber:* Zum Lieferumfang von Livelink WCM Server gehört der Treiber für bestimmte Versionen des RDBMS Oracle. Dieses Feld wird nur aktiv, wenn Sie ein anderes RDBMS oder eine andere Version des RDBMS Oracle verwenden. In dem Fall wählen Sie hier die Datei(en) mit den JDBC-Treibern für die verwendete Datenbank aus.

  Die Dateien werden mit vollständigem Pfad in das Feld übernommen, mehrere Pfade werden durch Semikolon getrennt.

  Das Installationsprogramm kopiert diese Datei(en) in das Verzeichnis **{WCM-Installationsverzeichnis}\external_lib**. Dies erfolgt auf allen Servern. Informationen zu JDBC-Treibern für Datenbanken erhalten Sie beim jeweiligen Hersteller.

Hinweise

- Verwenden Sie immer die JDBC-Treiber, die zur aktuellen Version der Datenbank und zum benutzten Java SDK passen. Bei der Aktualisierung der Version (z.B. durch ein Fixpack) kann sich auch die Version des JDBC-Treibers ändern. Ersetzen Sie bei Verwendung von MS SQL Server 2000 in einem solchen Fall die entsprechenden Dateien im Verzeichnis **{WCM-Installationsverzeichnis}\external_lib**, und starten Sie die entsprechenden Server neu.
- Haben Sie einen Oracle-Patch installiert, der einen neuen JDBC-Treiber enthält, tauschen Sie nach der Installation des Patches die Treiber-Datei (z.B. **classes12.zip**) im Verzeichnis **{WCM-Installationsverzeichnis}\external_lib** gegen die aktuelle Datei aus.
- Falls sich der Name der Treiberklasse nachträglich ändert, muss ein neuer Pool für die Verbindung zur Datenbank eingerichtet und den entsprechenden Servern zugeordnet werden.

- *JDBC-Treiber:* Treiberklasse für das verwendete RDBMS

  Wenn Sie Oracle als Datenbanktyp ausgewählt haben, wird der Name der Treiberklasse automatisch eingestellt.

  Verwenden Sie ein anderes RDBMS, tragen Sie den Namen der Treiberklasse ein. Nutzen Sie z.B. den JDBC-Treiber von Microsoft für das RDBMS MS SQL Server 2000, tragen Sie hier `com.microsoft.jdbc.sqlserver.SQLServerDriver` ein. Weitere Informationen erhalten Sie in der Dokumentation zum verwendeten JDBC-Treiber.

Bereich *Verbindungsdaten*

- *Datenquelle:* vollständige Bezeichnung der Datenquelle

  Wenn Sie das RDBMS Oracle verwenden, klicken Sie auf die Schaltfläche ..., um im darauf folgenden Dialog *JDBC-Datenquelle* die genauen Parameter für die Verbindung zum RDBMS einzustellen.

  - *Datenbankhost:* voll qualifizierter Hostname oder IP-Adresse des Rechners, auf dem sich die Datenbank befindet
  - *Datenbank-Port:* Port der Datenbank für die Verbindung. Hier wird automatisch der Standardwert für den ausgewählten Datenbanktyp eingetragen.
  - *Datenbankname:* Name der Datenbank

  Wenn Sie ein anderes RDBMS verwenden, tragen Sie die URL für den Zugriff auf das RDBMS in das Feld ein. Das Format der URL ist abhängig vom verwendeten JDBC-Treiber. Für den JDBC-Treiber von Microsoft für das RDBMS MS SQL Server 2000 ist hier z.B. Folgendes einzutragen:
  `jdbc:microsoft:sqlserver://{Datenbankhost}:1433;SelectMethod=cursor;DatabaseName={Datenbank-Name}`. Weitere Informationen erhalten Sie in der Dokumentation zum verwendeten JDBC-Treiber.

- *Eigentümer* (nur für SQL Server): Kennung des Benutzers, der die von Livelink WCM Server benutzten Datenbankobjekte im RDBMS angelegt hat
- *Benutzer:* Benutzerkennung für den Zugriff auf das RDBMS. Bei Verwendung des RDBMS Oracle darf diese Benutzerkennung keine Bindestriche enthalten.
- *Passwort:* Passwort für den Zugriff auf das RDBMS

Prüfen Sie anschließend die Datenbankverbindung durch Klicken auf die Schaltfläche *Testen*. Wenn alle Angaben korrekt vorgenommen wurden, wird die Überprüfung mit *OK* bestätigt. In dem Fall können Sie sich durch Klicken auf die Schaltfläche *Details* Informationen zum verwendeten RDBMS und JDBC-Treiber anzeigen lassen.

Bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Weiter*.

Parameter des Livelink-Systems einstellen

Wenn Sie bei der Einrichtung des Admin-Servers unter *Benutzerverwaltung* das Optionsfeld *Livelink* aktiviert haben, sind im nächsten Dialog die Parameter für die Verbindung zum Livelink-System festzulegen.

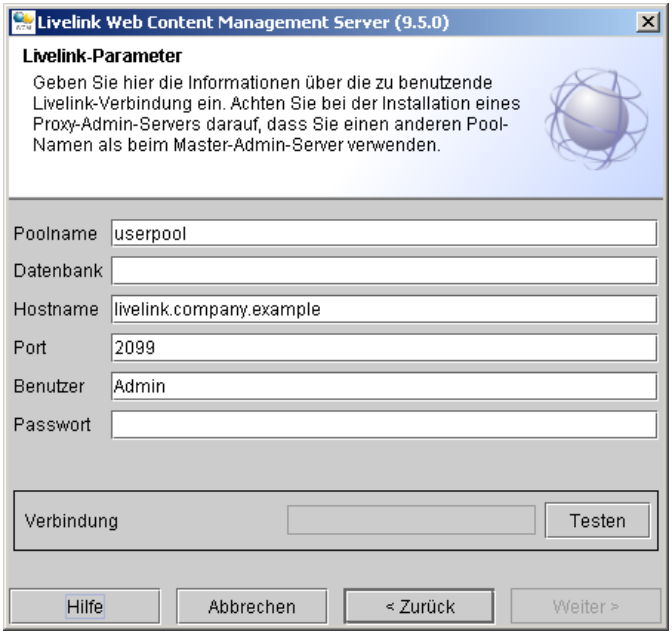


Abb. 9 – Parameter des zu benutzenden Livelink-System

- *Poolname:* Name des Livelink-Pools, der für die Verbindung zum Livelink-System angelegt wird

  Achtung! Stellen Sie bei der Installation eines Proxy-Admin-Servers sicher, dass ein anderer Name als für den Pool des Master-Admin-Servers verwendet wird.

- *Datenbank:* logischer Name der Livelink-Datenbank, die verwendet werden soll. Im Normalfall bleibt das Feld leer, d.h., es wird die Datenbank benutzt, die im Livelink-System als Standard konfiguriert ist.
- *Hostname:* voll qualifizierter Hostname des Rechners, auf dem der Livelink-Server installiert ist
- *Port:* Port des Livelink-Servers für die Verbindung
- *Benutzer:* Benutzer für den Zugriff auf den Livelink-Server. Der Benutzer muss im Livelink-System Benutzer und Gruppen anlegen, ändern und löschen dürfen.
- *Passwort:* Passwort für den Zugriff auf den Livelink-Server

Prüfen Sie anschließend die Verbindung zum Livelink-System durch Klicken auf die Schaltfläche *Testen*. Wenn alle Angaben korrekt vorgenommen wurden, wird die Überprüfung mit *OK* bestätigt.

Parameter des LDAP-Verzeichnisdienstes einstellen

Wenn Sie bei der Einrichtung des Admin-Servers unter *Benutzerverwaltung* das Optionsfeld *LDAP* aktiviert haben, sind im nächsten Dialog die Parameter für die Verbindung zum LDAP-Verzeichnisdienst festzulegen.

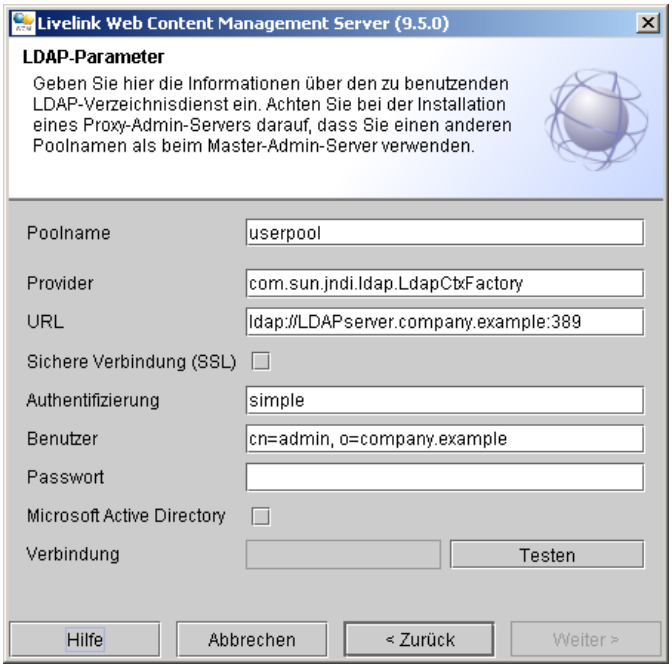


Abb. 10 – Parameter des zu benutzenden LDAP-Verzeichnisdienstes

Hinweis: Werden die Benutzer, die auf das WCM-System zugreifen sollen, in verschiedenen LDAP-Servern verwaltet, geben Sie hier den LDAP-Server an, in dem der zukünftige WCM-Administrator gespeichert ist. Nach der Installation können Sie über den Admin-Client zusätzliche LDAP-Pools für den Zugriff auf weitere LDAP-Server oder LDAP-Fallback-Server einrichten.

- *Poolname:* Name des LDAP-Pools, der für die Verbindungen zum LDAP-Server angelegt wird

  Achtung! Stellen Sie bei der Installation eines Proxy-Admin-Servers sicher, dass ein anderer Name als für den Pool des Master-Admin-Servers verwendet wird.

- *Provider:* verwendeter Treiber für den LDAP-Server. Die hier angegebene Java-Klasse muss über den im System eingestellten Klassenpfad erreichbar sein. Die Standardklasse `com.sun.jndi.ldap.LdapCtxFactory` entspricht dem LDAP-Standard und kann für LDAP-Verzeichnisdienste verschiedener Hersteller verwendet werden.

- *URL:* Adresse des LDAP-Servers, zusammengesetzt aus dem Protokoll ldap://, dem Namen des LDAP-Servers und dem Port für LDAP-Verbindungen (Standard = 389)
  Beispiel: “ldap://LDAPserver.company.example:389”

- *Sichere Verbindung (SSL):* Aktivieren Sie dieses Kontrollkästchen, wenn die Kommunikation zum LDAP-Server über gesicherte Verbindungen (Secure Socket Layer) erfolgt.

  Wenn Sie SSL verwenden möchten, muss das LDAP-Serverzertifikat vor der Installation dem WCM-Truststore hinzugefügt werden (siehe Abschnitt 3.5 “SSL-Verbindung zum LDAP-Server verwenden” auf Seite 64).

- *Authentifizierung:* Authentifizierungsmethode für die Anmeldung am LDAP-Server. Hier muss die Methode “simple” eingetragen werden.
- *Benutzer:* Benutzername des Bindeprofils für den Zugriff auf den LDAP-Verzeichnisdienst. Geben Sie den “distinguished name” des Benutzers an.

  Beachten Sie die Hinweise zum Bindeprofil im Abschnitt “LDAP-Bindeprofil einrichten” auf Seite 57.
- *Passwort:* Passwort des Bindeprofils

  Achtung! Bei Änderung des Passworts im LDAP-Verzeichnisdienst ist eine Anbindung des WCM-Systems an den LDAP-Verzeichnisdienst nicht mehr möglich.
- *Microsoft Active Directory:* Aktivieren Sie dieses Kontrollkästchen, wenn Sie Microsoft Active Directory verwenden.

Prüfen Sie anschließend die Verbindung zum LDAP-Server durch Klicken auf die Schaltfläche *Testen*. Wenn alle Angaben korrekt vorgenommen wurden, wird die Überprüfung mit *OK* bestätigt.

Bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Weiter*.

WCM-spezifische LDAP-Parameter angeben

Livelink WCM Server benötigt eigene Objektklassen im LDAP-Verzeichnisdienst, die vor der Installation in LDAP hinzugefügt werden müssen (siehe Abschnitt 3.2 “Zusätzliche Objektklassen und Attribute einrichten” ab Seite 40). Geben Sie in diesem Dialog die Namen dieser Objektklassen an.

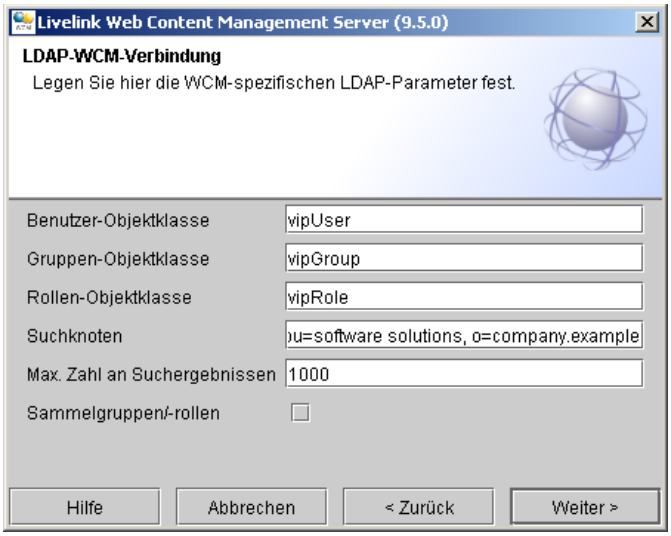


Abb. 11 – WCM-spezifische LDAP-Parameter

- *Benutzer-Objektklasse:* Objektklasse zum Speichern der Benutzerinformationen. Der Standardname ist `vipUser` (für Microsoft Active Directory `user`).
- *Gruppen-Objektklasse:* Objektklasse zum Speichern der Gruppeninformationen. Der Standardname ist `vipGroup` (für Microsoft Active Directory `group`).
- *Rollen-Objektklasse:* Objektklasse zum Speichern der Rolleninformationen. Der Standardname ist `vipRole` (für Microsoft Active Directory `group`).
- *Suchknoten:* Wurzel-Namenskontext (base DN), ab dem das WCM-System lesend und schreibend auf den LDAP-Namensraum zugreifen kann. Der Suchknoten kann sich z. B. aus der Organisation (o) und der Organisationseinheit (ou) zusammensetzen.

Beispiel: “o=company.example, ou=marketing”
Alle Einträge in den Namensräumen in und unterhalb von “marketing” sind nun von Livelink WCM Server aus zugreifbar.

- *Max. Zahl an Suchergebnissen:* maximale Anzahl an Ergebnissen, die bei einer Suche im LDAP-Verzeichnisdienst von Livelink WCM Server abgeholt wird. Abhängig vom verwendeten Produkt kann im LDAP-Server konfiguriert werden, wie viele Suchergebnisse geliefert werden. Die maximale Zahl an Suchergebnissen, die für Livelink WCM Server konfiguriert ist, sollte kleiner oder gleich der maximalen Anzahl von gelieferten Suchergebnissen sein, die im LDAP-Server eingestellt ist.

  Wenn Sie hier keinen Wert eintragen, wird der Standardwert 1000 verwendet.

  Beispiel: Im LDAP-Verzeichnisdienst Microsoft Active Directory wird die maximale Zahl zurückgelieferter Suchergebnisse über den Parameter `MaxPageSize` gesteuert. Dieser Parameter gehört zu dem Attribut `LDAPAdminLimits` der Query-Policies von Active Directory. Die Query-Policies können z.B. mithilfe des Tools **Ntdsutil.exe** bearbeitet werden. Auf die Query-Policies kann außerdem über den LDAP-Konfigurationskontext zugegriffen werden, der z.B. folgendermaßen lauten kann: `CN=Default Query Policy,CN=Query-Policies,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=win2000,DC=de`.

- *Sammelgruppen/-rollen:* Mit dieser Option können Sie festlegen, dass implizite Zuordnungen von Benutzern zu Gruppen und Rollen im WCM-System berücksichtigt werden (siehe Abschnitt 3.1 “Konzept der Sammelgruppen und Sammelrollen” auf Seite 38).

> **Hinweis:** Die Einstellung, die Sie hier vornehmen, gilt als globale Einstellung für den gesamten LDAP-Pool. Wenn Sie in Ihrem WCM-System mehrere LDAP-Pools eingerichtet haben, stellen Sie sicher, dass diese Einstellung für Pools, deren LDAP-Kontexte sich überschneiden, identisch ist.

- *Wert des Attributs vipType für ...:* Wenn Sie im vorangegangenen Dialog das Kontrollkästchen *Microsoft Active Directory* aktiviert haben, wird Ihnen zusätzlich dieser Bereich angezeigt. Hier können Sie für die Principal-Typen *Benutzer*, *Gruppe* und *Rolle* den jeweiligen Wert des Attributs `vipType` spezifizieren. Dies ist z.B. hilfreich, wenn Sie die Benutzerinformationen aus Ihrem LDAP-Verzeichnisdienst für mehrere installierte WCM-Systeme verwenden. Mithilfe dieses Attributs lässt sich der Zugriff auf die einzelnen WCM-Systeme separat steuern.

Bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Weiter*.

WCM-Administrator einrichten

In diesem Dialog geben Sie Benutzerkennung und Passwort des WCM-Administrators an. Dieser Benutzer erhält damit initial den vollen Zugriff auf den Admin-Client. Im Admin-Client können Sie später weiteren Benutzern Administrationsrechte gewähren.

Abhängig von der Art Ihrer Benutzerverwaltung (siehe Abschnitt “Parameter des neuen Administrationsservers einstellen” auf Seite 79) muss der Benutzer folgenden Bedingungen genügen:

- *RDBMS:* Geben Sie eine Benutzerkennung an, die noch nicht in der Datenbank vorhanden ist.

- *LDAP:* Geben Sie eine Benutzerkennung an, die bereits im LDAP-Verzeichnisdienst vorhanden ist. Achten Sie darauf, dass hier ein anderer Benutzer als beim LDAP-Bindeprofil eingetragen wird (siehe Abschnitt 3.3 “LDAP-Bindeprofil und WCM-Administrator einrichten” ab Seite 56).
- *Livelink:* Geben Sie eine Benutzerkennung an, die bereits in Livelink vorhanden ist. Der Benutzer muss im Livelink-System Benutzer und Gruppen anlegen, ändern und löschen dürfen.

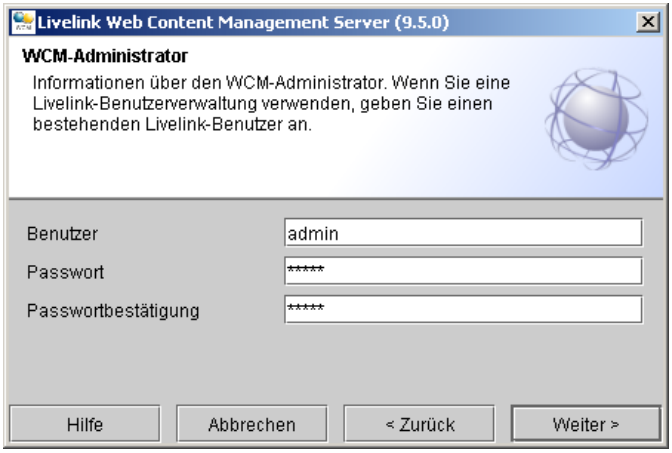


Abb. 12 – WCM-Administrator einrichten

Wenn Sie die Benutzerdaten in einer Datenbank verwalten, tragen Sie in den übrigen Feldern das entsprechende Administratorpasswort ein. Wenn Sie einen LDAP-Server oder eine Livelink-Benutzerverwaltung verwenden, entfällt die Angabe eines Passworts.

Bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Weiter*.

Installationsprozess fertig stellen oder weitere Server hinzufügen?

Im nächsten Dialog können Sie entscheiden, ob Sie den Installationsprozess mit der Installation des Administrationsservers fertig stellen oder ob Sie zum System noch weitere Server hinzufügen möchten.

- *Admin-Server installieren:* Wenn Sie das System mit den bis jetzt vorgenommen Einstellungen installieren möchten, aktivieren Sie dieses Optionsfeld.

  In diesem Fall wird nur der Administrationsserver eingerichtet, weitere Server können Sie mithilfe des Installationsprogramms zu einem späteren Zeitpunkt einrichten.

  Im nächsten Dialog werden Ihnen die zu installierenden Komponenten zur Überprüfung angezeigt. Um die Installation zu starten, bestätigen Sie die Angaben durch Klicken auf die Schaltfläche *Fertig*.

- *Weitere Server zum WCM-System hinzufügen*: In der Regel werden beim Installationsprozess noch weitere Komponenten installiert. Lassen Sie in diesem Fall die Standard-Option aktiviert, und fahren Sie durch Klicken auf die Schaltfläche *Weiter* fort.

Option für die Serverinstallation auswählen

Für die Installation weiterer Server müssen Sie nun angeben, wie Ihr WCM-System aufgebaut sein soll.

Livelink Web Content Management Server (9.5.0)
Optionen für die Serverinstallation
Legen Sie hier die grundsätzliche Vorgehensweise für die Installation der Content-Server fest.
Minimalinstallation
Bei der Minimalinstallation besteht Ihr WCM-System aus einem Master-Admin-Server und einem Master-Content-Server.
Benutzerdefinierte Installation
Die benutzerdefinierte Installation ermöglicht einen individuellen Aufbau Ihres WCM-Systems, sodass Sie die einzelnen Server bzw. Komponenten des Systems Ihren Anforderungen entsprechend installieren können.
Hilfe
Abbrechen
< Zurück
Weiter >

Abb. 13 – Installationsvarianten

> **Hinweis:** Allgemeine Informationen zur Architektur von WCM-Systemen erhalten Sie im Livelink WCM Server-Administratorhandbuch (Kapitel “Konzepte”).

Aktivieren Sie das gewünschte Optionsfeld, und klicken Sie auf die Schaltfläche *Weiter*.

Server einrichten

Der Dialog zum Einrichten der Content-Server wird geöffnet. Dieser Dialog enthält ein Register für den Master-Content-Server.

Abb. 14 – Dialog zum Einrichten der Server

Hinweise:

Für die Bearbeitung der WCM-Objekte über den Content-Client wird mindestens ein Content-Server benötigt, der im Kontext der JSP-Engine bzw. als Webanwendung im Application-Server läuft.

Wenn Sie mehrere in der JSP-Engine laufende Content-Server auf demselben Rechner einrichten, müssen unterschiedliche JSP-Engines zum Ausführen der Server verwendet werden. Passen Sie in diesem Fall nach der Installation von Livelink WCM Server in den Skripten zum Starten der entsprechenden Content-Server die eingerichtete Standard-URL entsprechend der Konfiguration der verwendeten JSP-Engine an (siehe Abschnitt “Content-Server im Application-Server starten” auf Seite 170).

Machen Sie für den Server die erforderlichen Angaben:

- *Name:* Name des Servers. Dieser Name ist frei wählbar, muss jedoch innerhalb des WCM-Systems eindeutig sein. Folgende Zeichen sind erlaubt:
  - a–z, A–Z, 0–9 (ASCII 7 Bit)
  - . (Punkt), _ (Unterstrich) und - (Bindestrich)
- *Hostname:* voll qualifizierter Hostname des Rechners, auf dem dieser Server installiert werden soll

  Standardmäßig wird versucht, den Namen des aktuellen Rechners zu ermitteln. Wenn das nicht möglich ist, wird der Standardeintrag “localhost” eingetragen. Dieser Eintrag sollte jedoch geändert werden, da er bei verteilten Systemen zu Problemen führt.
- *VIPP-Port* und *HTTP-Port:* Port-Nummern des Servers für die Verbindung über das Protokoll VIPP bzw. HTTP. Das Installationsprogramm legt einen Pool für die Verbindungen zu diesem Server an, der den Namen des entsprechenden Servers erhält.

Hinweise:

Achten Sie darauf, dass die angegebenen Port-Nummern nicht von anderen Anwendungen verwendet werden. Sind zwischen den einzelnen Servern oder zwischen Client und Server Firewalls vorhanden, sind die entsprechenden Port-Adressen freizuschalten.

Nach der Installation können Sie über den Admin-Client weitere Parameter für die Kommunikation über das entsprechende Protokoll festlegen (Ansicht *Konfiguration* → *Pools* → *WCM* → *{Poolname}* → Registerkarte *WCM-Verbindung*).

- *SSL:* Durch Aktivieren des Kontrollkästchens *SSL* können Sie festlegen, dass die Kommunikation zwischen den Servern über gesicherte Verbindungen (Secure Socket Layer) erfolgt.
- *Encoding* (nur für in der JSP-Engine oder im Application-Server laufende Content-Server): Wählen Sie ein Encoding für den Content-Server und damit für den Content-Client aus.

  Verwenden Sie UTF-8 codierte Seiten (Unicode) in Ihrer Website, wählen Sie *UTF-8* aus. Benötigen Sie keine Unicode-Unterstützung, wählen Sie *ISO-8859-1*.

  Hinweis: Das Encoding muss für alle Komponenten des WCM-Systems konsistent eingestellt sein. Bitte beachten Sie die Hinweise zur Verwendung von Unicode im Livelink WCM Server-Administratorhandbuch (Kapitel “Konzepte”).

- *Dienst einrichten* (nicht für in der JSP-Engine oder im Application-Server laufende Content-Server): Mit dieser Option können Sie für den Server unter Windows einen Dienst zum automatischen Starten und Beenden des Servers einrichten.

> **Hinweis:** Mithilfe der Skripte **install_{Servername}.bat** im Verzeichnis **{WCM-Installationsverzeichnis}\installation\service** können Sie auch nach der Installation Dienste für die Server einrichten.

- *Serverkategorie:* Die Serverkategorie wird automatisch vorgeschlagen.

  Allgemeine Informationen zu Serverkategorien enthält das Livelink WCM Server-Administratorhandbuch.

- *Webanwendung erzeugen:* Um mit dem Content-Client bzw. dem Content-Client (Classic) arbeiten zu können, muss mindestens einer der Content-Server im Kontext einer JSP-Engine oder als Webanwendung in einem Application-Server ausgeführt werden.

  Wenn Sie für den Server eine Webanwendung erzeugen möchten, aktivieren Sie dieses Kontrollkästchen, und klicken Sie auf die Schaltfläche ... . Eine Beschreibung der einzustellenden Parameter finden Sie im folgenden Abschnitt.

Mit diesen Einstellungen sind die erforderlichen Angaben für die Minimalinstallation abgeschlossen. Führen Sie einen der folgenden Schritte aus:

- Um weitere Server hinzuzufügen, klicken Sie auf die Schaltfläche *Server hinzufügen*. Es öffnet sich ein neues Register, auf dem Sie die für diesen Server erforderlichen Parameter eingeben können.
- Um die Einträge für einen Server wieder zu entfernen, gehen Sie auf das entsprechenden Register, und klicken Sie auf die Schaltfläche *Server entfernen*.
- Wenn Sie alle Servereinstellungen abgeschlossen haben, klicken Sie auf die Schaltfläche *Weiter*.

Webanwendung erzeugen

Wenn Sie das Kontrollkästchen *Webanwendung erzeugen* aktivieren und die Schaltfläche ... klicken, öffnet sich der Dialog *Webanwendung erzeugen*.

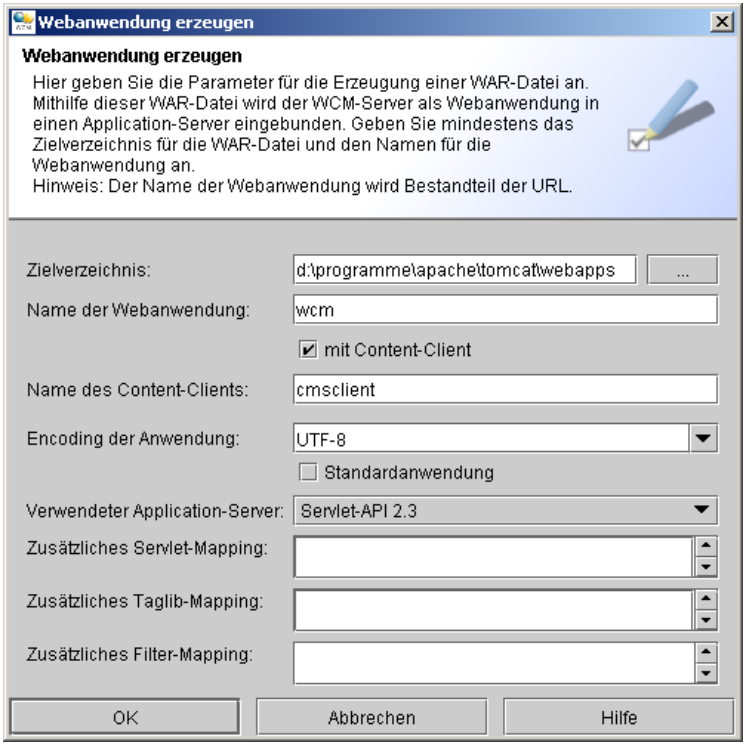


Abb. 15 – Webanwendung für einen Content-Server erzeugen

Machen Sie hier die erforderlichen Angaben:

- *Zielverzeichnis:* Verzeichnis, in dem die erzeugte WAR-Datei gespeichert werden soll. Dies ist meist das Webanwendungsverzeichnis des Application-Servers.
- *Name der Webanwendung:* Name für die erzeugte Webanwendung. Dieser Name bestimmt den Dateinamen der WAR-Datei und wird Bestandteil der URL, über die die Webanwendung im Application-Server aufgerufen wird.

  Beispiel: Sie erzeugen eine Webanwendung für den Master-Content-Server. Als Namen der Webanwendung geben Sie “wcm” an. Die erzeugte WAR-Datei heißt dementsprechend **wcm.war**. Der Ausdruck “wcm” wird an die Basis-URL des Application-Servers angefügt, sodass die Webanwendung für den Master-Content-Server über die URL “http://wcmserver.company.example/wcm” aufgerufen wird.
- *mit Content-Client:* Aktivieren Sie dieses Kontrollkästchen, um den Content-Client ebenfalls in die Webanwendung einzubinden.

  Analog zum Namen der Webanwendung wird auch der Name des Content-Clients an die URL angefügt, sodass er z.B. über die Adresse “http://wcmserver.company.example/wcm/cmsclient” gestartet werden kann.

  Hinweis: Zum Lieferumfang von Livelink WCM Server gehören sowohl der Content-Client als auch sein Vorgänger, der Content-Client (Classic). Wenn Sie das Kontrollkästchen *Mit Content-Client* aktivieren, werden beide Clients in die Webanwendung eingebunden. Für den Content-Client (Classic) wird automatisch der Name “htmlclient” verwendet. Der Content-Client (Classic) kann dann beispielsweise über die Adresse “http://wcmserver.company.example/wcm/htmlclient” aufgerufen werden.

- *Encoding der Anwendung:* Wählen Sie ein Encoding für die erzeugte Webanwendung aus. Ist Ihre Website auf UTF-8 (Unicode) eingestellt, wählen Sie “UTF-8” aus der Liste. Unicode wird für die Darstellung osteuropäischer und asiatischer Sprachen benötigt, für westeuropäische Sprachen ist das Encoding “ISO-8859-1” (entspricht Latin-1) ausreichend. Der Application-Server muss entsprechend konfiguriert sein.
- *Standardanwendung:* Wenn Sie dieses Kontrollkästchen aktivieren, wird vorausgesetzt, dass die erzeugte Webanwendung im Application-Server als Standardanwendung (default application) definiert ist. Die Standardanwendung wird über die Root-URL des Application-Servers angesprochen, d.h., die URL enthält nicht den Anwendungsnamen. Der Content-Client würde in diesem Fall direkt über “http://wcmserver.company.example/cmsclient” aufgerufen werden. Die Definition als Standardanwendung erfolgt über die Konfiguration der Anwendung im Application-Server.
- *Verwendeter Application-Server:* Wählen Sie den verwendeten Application-Server aus der Liste. Die erzeugte WAR-Datei wird an die Erfordernisse des entsprechenden Produkts angepasst.

  Alternativ zu einem Produkt können Sie einen Servlet-API-Standard aus der Liste wählen: 2.2 oder 2.3. In diesem Fall wird die WAR-Datei entsprechend der Java Servlet Specification erzeugt.
- *Zusätzliches Servlet-, Taglib- und Filter-Mapping:* Die in Livelink WCM Server verwendeten Servlets, Tag Libraries und Filter-Servlets werden automatisch gemappt. Dabei werden die von den Servlets verwendeten Java-Klassen auf URLs gemappt. Bei der Verwendung von Tag Libraries wird über das Mapping der Pfad zu den verwendeten TLD-Dateien angegeben.

Falls Sie darüber hinaus weitere Servlets, Tag Libraries oder Filter-Servlets verwenden, die auch in der erzeugten Webanwendung verfügbar sein sollen, tragen Sie hier das entsprechende Mapping ein.

Beispiel für ein Servlet-Mapping

```
<servlet>
   <servlet-name>MyServlet</servlet-name>
   <servlet-class>com.company.MyServlet</servlet-class>
</servlet>
<servlet-mapping>
   <servlet-name>MyServlet</servlet-name>
   <url-pattern>/servlet/MyServletAlias</url-pattern>
</servlet-mapping>
```

Beispiel für ein Taglib-Mapping

```
<taglib>
   <taglib-uri>
      myTaglet.tld
   </taglib-uri>
   <taglib-location>
      /WEB-INF/tld/myTaglet.tld
   </taglib-location>
</taglib>
```

Beispiel für ein Filter-Mapping

```
<filter>
   <filter-name>MyFilter</filter-name>
   <filter-class> com.company.MyFilter</filter-class>
</filter>
<filter-mapping>
   <filter-name>MyFilter</filter-name>
   <url-pattern>/filter/MyFilterAlias</url-pattern>
</filter-mapping>
```

Suchserver einrichten

Wenn Sie eine Lizenz für Content Miner oder den Search Server Connector für Lucene besitzen, wird der Dialog zum Einrichten von Suchservern geöffnet. Dieser Dialog enthält die drei Register *Content Miner*, *Lucene* und *Livelink*. Auf diesen Registern können Sie nun die gewünschte Anzahl von Suchservern hinzufügen.

Register *Content Miner*

> **Hinweis:** Allgemeine Informationen zu den Konzepten von Content Miner entnehmen Sie bitte dem Content Miner-Handbuch.

Klicken Sie auf die Schaltfläche *Suchserver hinzufügen*. Ein Register wird eingeblendet, auf dem Sie die Angaben zum Content Miner-Suchserver eintragen können.

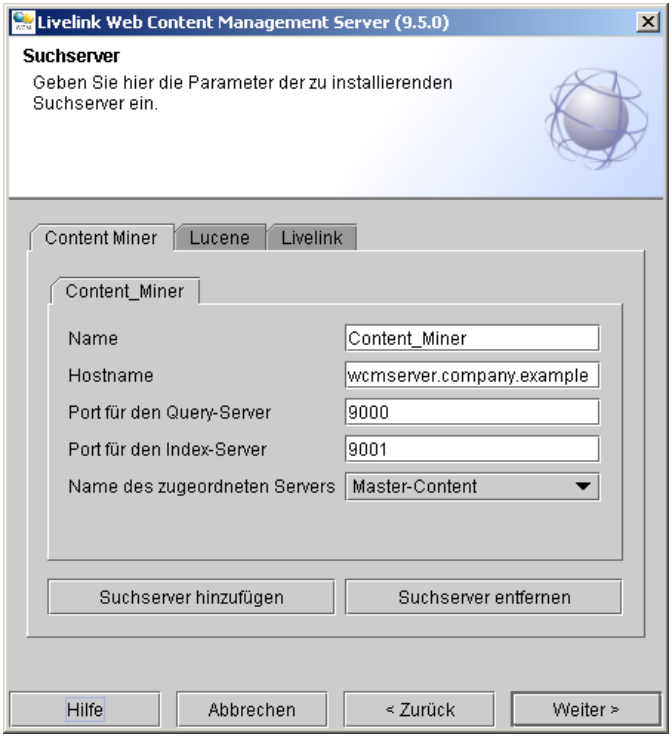


Abb. 16 – Installation eines Content Miner-Suchservers

- *Name:* Name des Servers. Dieser Name ist frei wählbar, muss jedoch innerhalb des WCM-Systems eindeutig sein. Folgende Zeichen sind erlaubt:
  - a–z, A–Z, 0–9 (ASCII 7 Bit)
  - . (Punkt), _ (Unterstrich) und - (Bindestrich)
- *Hostname:* voll qualifizierter Hostname des Rechners, auf dem dieser Server installiert werden soll
- *Port für den Query-Server:* Port des Query-Servers für die Verbindung

Die Standardeinstellung ist 9000. Achten Sie darauf, dass der Port nicht von anderen Anwendungen bzw. Suchservern verwendet wird.

- *Port für den Index-Server:* Port des Index-Servers für die Verbindung

  Die Standardeinstellung ist 9001. Achten Sie auch hier darauf, dass der Port nicht von anderen Anwendungen bzw. Suchservern verwendet wird.

- *Name des zugeordneten Servers:* Name eines vorhandenen bzw. zu installierenden Content-Servers, dem dieser Suchserver zugeordnet werden soll

> **Hinweise:**
>
> Diese Zuordnung ist nachträglich nicht änderbar. Um einen Suchserver einem anderen Content-Server zuzuordnen, müssen Sie den Suchserver zunächst deinstallieren, anschließend erneut installieren und dem gewünschten Server zuordnen.
>
> Damit der Suchserver automatisch zusammen mit dem zugeordneten Content-Server startet und stoppt und über den Admin-Client gestartet und gestoppt werden kann, müssen Server und Suchserver auf demselben Hostrechner installiert sein (siehe Abschnitt “Suchserver starten” auf Seite 172).

Um einen weiteren Suchserver hinzufügen, klicken Sie erneut auf die Schaltfläche *Suchserver hinzufügen*. Ein neues Register wird hinzugefügt, auf dem Sie den nächsten Suchserver konfigurieren können.

Wenn Sie die Einträge für einen Suchserver wieder löschen möchten, wählen Sie das entsprechende Register und klicken anschließend auf die Schaltfläche *Suchserver entfernen*. Sämtliche Einstellungen werden auf diese Weise gelöscht.

Register *Lucene*

> **Hinweis:** Allgemeine Informationen zu den Konzepten von Lucene entnehmen Sie bitte dem Handbuch zum Search Server Connector für Lucene.

Klicken Sie auf die Schaltfläche *Suchserver hinzufügen*. Ein Register wird eingeblendet, auf dem Sie die Angaben zum Lucene-Suchserver eintragen können.

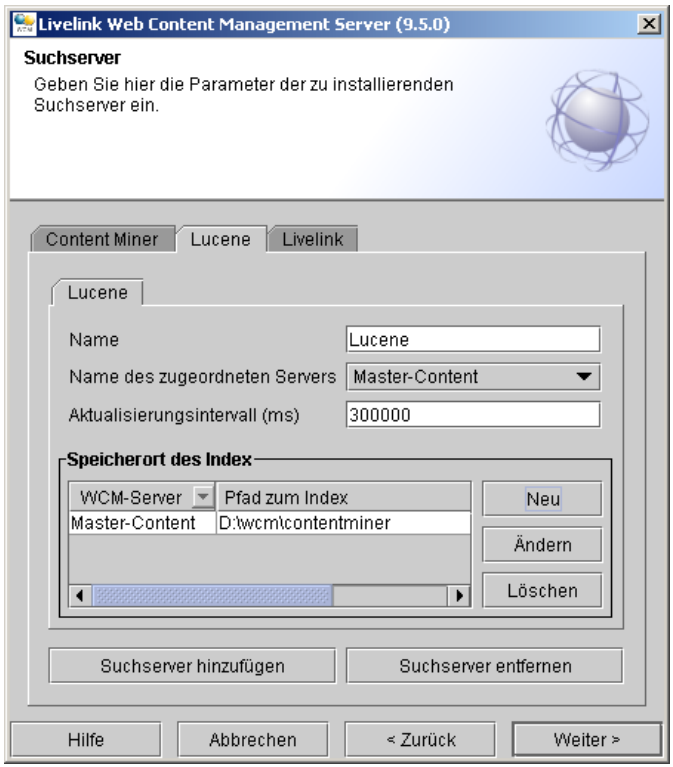


Abb. 17 – Installation eines Lucene-Suchservers

- *Name:* Name des Servers. Dieser Name ist frei wählbar, muss jedoch innerhalb des WCM-Systems eindeutig sein. Folgende Zeichen sind erlaubt:
  - a–z, A–Z, 0–9 (ASCII 7 Bit)
  - . (Punkt), _ (Unterstrich) und - (Bindestrich)
- *Name des zugeordneten Servers:* Name eines vorhandenen bzw. zu installierenden Content-Servers, dem dieser Suchserver zugeordnet werden soll

> **Hinweis:** Lucene-Suchserver müssen im gleichen Verzeichnis wie der zugeordnete Content-Server installiert werden. Diese Auswahlliste enthält nur die Server, die diese Voraussetzung erfüllen.

- *Aktualisierungsintervall (ms):* Zeitspanne in Millisekunden, nach der alle Collections für den lesenden Zugriff neu geladen werden
- *Speicherort des Index:* In diesem Bereich geben Sie den Pfad zu dem Verzeichnis im Dateisystem an, in dem der Index gespeichert ist. Dieser Speicherort muss von allen Servern erreichbar sein.

> **Hinweis:** Den Speicherort stellen Sie für jeden Server individuell ein, wobei die jeweiligen Pfade für alle Server auf das gleiche Verzeichnis zeigen müssen. Befindet sich ein Server auf einem anderen Hostrechner, muss das Verzeichnis auf beiden Hostrechnern gemountet sein.

  - *Neu:* Um einen neuen Pfad zum Index einzustellen, klicken Sie auf die Schaltfläche *Neu*. Es öffnet sich ein Dialog, in dem Sie einen Server auswählen und den entsprechenden Pfad zum Index eintragen.

- *Ändern:* Um den Eintrag für einen Server zu bearbeiten, markieren Sie den entsprechenden Server, und klicken Sie auf die Schaltfläche *Ändern*.
- *Löschen:* Um einen Eintrag zu entfernen, markieren Sie den entsprechenden Server, und klicken Sie auf die Schaltfläche *Löschen*.

Um einen weiteren Suchserver hinzufügen, klicken Sie erneut auf die Schaltfläche *Suchserver hinzufügen*. Ein neues Register wird hinzugefügt, auf dem Sie den nächsten Suchserver konfigurieren können.

Wenn Sie die Einträge für einen Suchserver wieder löschen möchten, wählen Sie das entsprechende Register und klicken anschließend auf die Schaltfläche *Suchserver entfernen*. Sämtliche Einstellungen werden auf diese Weise gelöscht.

Register *Livelink*

Hinweis: Informationen zur Einbindung und Verwendung der Livelink-Suche in einem WCM-System entnehmen Sie bitte dem Livelink-Integrationshandbuch.

Klicken Sie auf die Schaltfläche *Suchserver hinzufügen*. Ein Register wird eingeblendet, auf dem Sie die Angaben zum Livelink-Suchserver eintragen können.

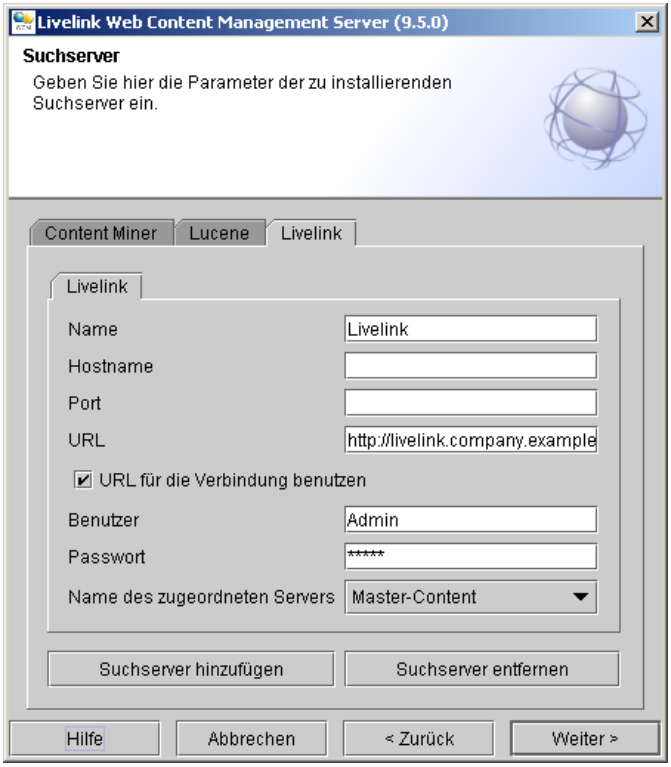


Abb. 18 – Installation eines Livelink-Suchservers

- *Name:* Name des Servers. Dieser Name ist frei wählbar, muss jedoch innerhalb des WCM-Systems eindeutig sein. Folgende Zeichen sind erlaubt:
  - a–z, A–Z, 0–9 (ASCII 7 Bit)
  - . (Punkt), _ (Unterstrich) und - (Bindestrich)
- *Hostname:* voll qualifizierter Hostname des Rechners, auf dem der Livelink-Server installiert ist, der die Indexierung durchführen und die Suchanfragen bearbeiten soll

- *Port:* Port des Livelink-Servers für die Verbindung
- *URL:* URL zum Livelink-Server, der die Indexierung durchführen und die Suchanfragen beantworten soll. Die URL ist vom Typ http://livelink.company.example/livelink/livelink.exe.
- *URL für die Verbindung benutzen:* Aktivieren Sie dieses Kontrollkästchen, wenn Sie für die Verbindung zum Livelink-Server dessen URL verwenden möchten. Die Einträge in den Feldern *Hostname* und *Port* werden in diesem Fall nicht berücksichtigt.
- *Benutzer:* Benutzer für die Bearbeitung der Suchanfragen im Livelink-System. Der Benutzer muss lesend auf die Segmente (Collections) zugreifen können.

  Hinweise:

  Sie können für die Livelink-Suche festlegen, welche Indexattribute abfragbar bzw. anzeigbar sein sollen. Diese Einstellungen sind benutzerspezifisch. Es empfiehlt sich daher, einen speziellen Benutzer für die Livelink-Suche anzulegen, den Sie anschließend hier angeben.

  Informationen zu den Berechtigungen bei der Livelink-Suche erhalten Sie im Livelink-Integrationshandbuch (Kapitel “Livelink-Suche im WCM-System”).

- *Passwort:* Passwort für die Bearbeitung der Suchanfragen im Livelink-System
- *Name des zugeordneten Servers:* Name eines vorhandenen bzw. zu installierenden Content-Servers, dem dieser Suchserver zugeordnet werden soll

Um einen weiteren Suchserver hinzufügen, klicken Sie erneut auf die Schaltfläche *Suchserver hinzufügen*. Ein neues Register wird hinzugefügt, auf dem Sie den nächsten Suchserver konfigurieren können.

Wenn Sie die Einträge für einen Suchserver wieder löschen möchten, wählen Sie das entsprechende Register und klicken anschließend auf die Schaltfläche *Suchserver entfernen*. Sämtliche Einstellungen werden auf diese Weise gelöscht.

Wenn Sie die Einstellungen für alle Suchserver abgeschlossen haben, klicken Sie auf die Schaltfläche *Weiter*.

Zusammenfassung der Komponenten

Im letzten Dialog des Installationsassistenten werden die zu installierenden Komponenten zusammenfassend angezeigt.

Bei einer Neuinstallation des WCM-Systems steht “Basissystem” an erster Stelle der Liste. Das Basissystem umfasst u. a. die Klassenbibliotheken von Livelink WCM Server und gemeinsam genutzte Dateien und Verzeichnisse der einzelnen Komponenten.

Um die Installation zu starten, klicken Sie auf die Schaltfläche *Fertig*.

Nach der Installation läuft der Administrationsserver bereits. Um die anderen Server zu starten, führen Sie die entsprechenden Startskripte aus, siehe Abschnitt “Server starten” auf Seite 163.

4.2 WCM-System benutzerdefiniert installieren

Die Beschreibung der benutzerdefinierten Installation des WCM-Systems lehnt sich an die Beschreibung eines verteilten Systems mit Firewall im Livelink WCM Server-Administratorhandbuch (Kapitel “Konzepte”) an. Das zu installierende WCM-System soll aus folgenden Komponenten bestehen und wie folgt aufgebaut sein:

- Hinter einer Firewall (d.h. im Intranet) befinden sich auf einem Rechner ein Master-Admin-Server und ein Master-Content-Server. Auf einem zweiten Rechner befindet sich ein Proxy-Content-Server, der als Webanwendung in einem Application-Server läuft. Über diesen Server erfolgt die Bearbeitung und Qualitätssicherung der WCM-Objekte mithilfe des Content-Clients.
- Vor der Firewall (d.h. außerhalb des Unternehmensnetzes) befinden sich ein Proxy-Content-Server, auf dem die Produktionssicht der Website veröffentlicht wird, und ein Proxy-Admin-Server. Der Proxy-Admin-Server wird vom Proxy-Content-Server für das Laden der Serverkonfiguration beim Starten, die Anmeldung von Benutzern am WCM-System und die Lizenzüberprüfung benötigt. Die Proxy-Server vor der Firewall greifen auf eine separate Datenhaltung zu.

Hinweis: Die Bereitstellung eines Proxy-Admin-Servers erfordert die separate Installation eines zweiten WCM-Systems vor der Firewall.

Gehen Sie bei der Installation dieses Szenarios wie folgt vor:

1. Master-WCM-System hinter der Firewall einrichten
2. Proxy-Content-Server hinter der Firewall einrichten
3. Proxy-WCM-System vor der Firewall einrichten

4. Proxy-Admin-Server in der Konfiguration des Master-Admin-Servers registrieren

Schritt 1 – Master-WCM-System hinter der Firewall einrichten

Zur Installation eines solchen Szenarios richten Sie zunächst auf einem Rechner hinter der Firewall, d.h. im Intranet, den Master-Admin- und den Master-Content-Server ein:

1. Gehen Sie wie in Abschnitt 4.1 “Neues WCM-System installieren (Minimalsystem)” ab Seite 72 beschrieben vor, und folgen Sie den Dialogen, wobei Sie den Master-Admin-Server einrichten.
2. Aktivieren Sie im Dialog *Optionen für die Serverinstallation* das Optionsfeld *Benutzerdefinierte Installation*.

   Hinweis: Es werden Ihnen keine Register zur Installation bestimmter Server angeboten. Mit Ausnahme des Administrationsservers werden alle Server über die Schaltfläche *Server hinzufügen* installiert.

3. Richten Sie für das WCM-System hinter der Firewall durch Klicken auf die Schaltfläche *Server hinzufügen* den Master-Content-Server ein.

   Genaue Angaben zu den einzelnen Parametern der Server finden Sie im Abschnitt “Server einrichten” auf Seite 97.

4. Bestätigen Sie die Servereinstellungen durch Klicken auf die Schaltfläche *Weiter*.
5. Falls Sie Suchserver einrichten möchten, nehmen Sie im folgenden Dialog die entsprechenden Einträge vor. Für die Installation von Content Miner bzw. Lucene-Suchservern benötigen Sie eine entsprechende Lizenz.

Genaue Angaben zum Einrichten von Suchservern finden Sie im Abschnitt “Suchserver einrichten” auf Seite 105.

Die zu installierenden Komponenten werden im abschließenden Dialog aufgelistet.

6. Um die Installation zu starten, klicken Sie auf die Schaltfläche *Fertig*.

Hinweis: Der Installationsvorgang wird abgebrochen, wenn der WCM-Administrator nicht erfolgreich angelegt oder wenn der Administrationsserver nicht gestartet oder erreicht werden konnte.

Schritt 2 – Proxy-Content-Server hinter der Firewall einrichten

Installieren Sie anschließend auf einem zweiten Rechner hinter der Firewall den Proxy-Content-Server. Gehen Sie dazu wie in Abschnitt 4.3 “Neue Server hinzufügen” ab Seite 118 beschrieben vor, und folgen Sie den Dialogen.

Schritt 3 – Proxy-WCM-System vor der Firewall einrichten

1. Installieren Sie ein weiteres WCM-System, und richten Sie den zweiten Administrationsserver als Proxy-Server ein. Dektivieren Sie dazu in dem Dialog mit den Daten des Administrationsservers das Kontrollkästchen *Master*, siehe Abschnitt “Parameter des neuen Administrationsservers einstellen” auf Seite 79.

   Auch für den Proxy-Admin-Server müssen Sie die Verbindung zu einer Benutzerverwaltung konfigurieren. Achten Sie darauf, dass Sie einen anderen Poolnamen als beim Master-Admin-Server angeben.

   Hinweise

   - Die Server des Proxy-Systems müssen eindeutige Namen besitzen, die im Master-System nicht verwendet werden.

- Master- und Proxy-Admin-Server sollten auf dieselbe Benutzerverwaltung zugreifen, d.h. denselben LDAP- oder Livelink-Server bzw. dieselbe Datenbank. Bei Verwendung einer Datenbank oder eines LDAP-Verzeichnisdienstes sind getrennte Server für die Benutzerverwaltung möglich, wenn die Datenbestände durch Synchronisation zwischen den Servern identisch gehalten werden. Diese Synchronisation ist **nicht** Aufgabe des WCM-Systems. Die getrennten Server müssen auf denselben Typ von Benutzerverwaltung zugreifen, z.B. beide auf eine Datenbank. Sie können nicht verschiedene Typen von Benutzerverwaltungen mischen.
- Der initiale Administrator des Proxy-WCM-Systems muss **dieselbe** Benutzerkennung haben wie der Administrator des Master-WCM-Systems.

2. Aktivieren Sie auch hier das Optionsfeld *Benutzerdefinierte Installation*, und richten Sie durch Klicken auf die Schaltfläche *Server hinzufügen* den Proxy-Content-Server ein.
3. Bestätigen Sie die Servereinstellungen durch Klicken auf die Schaltfläche *Weiter*.
4. Falls Sie Suchserver einrichten möchten, nehmen Sie im folgenden Dialog die entsprechenden Einträge vor. Für die Installation von Content Miner bzw. Lucene-Suchservern benötigen Sie eine entsprechende Lizenz.

> **Hinweis:** Beim Abgleich der Konfiguration von Proxy-Admin- und Master-Admin-Server werden die Suchserver-spezifischen Einstellungen des Proxy-Admin-Servers überschrieben. Bevor Sie die Suchserver konfigurieren (z.B. Collections anlegen), müssen Sie deshalb den Proxy-Admin-Server in der Konfiguration des Master-Admin-Servers registrieren (Funktion *Konfiguration abgleichen* im Admin-Client).

Der abschließende Dialog zeigt die zu installierenden Komponenten.

5. Um die Installation zu starten, klicken Sie auf die Schaltfläche *Fertig*.

Schritt 4 – Proxy-Admin-Server in der Konfiguration des Master-Admin-Servers registrieren

1. Starten Sie den Admin-Client auf dem Master-Admin-Server hinter der Firewall über das Skript **adminClient.bat** bzw. **adminClient.sh**.
2. Registrieren Sie den Proxy-Admin-Server in der Konfiguration des Master-Admin-Servers. Informationen zur genauen Vorgehensweise erhalten Sie im Livelink WCM Server-Administratorhandbuch.

   Der Content-Server vor der Firewall ist daraufhin im Master-System verfügbar. Achten Sie darauf, dass für die Kommunikation zwischen Master- und Proxy-System durch die Firewall die entsprechenden Ports freigeschaltet sind.

4.3 Neue Server hinzufügen

Sie können Ihrem WCM-System jederzeit neue Admin-Server, Content-Server und Suchserver hinzufügen, wenn sich beispielsweise die Anforderungen Ihres Unternehmens ändern.

Hinweise

- Voraussetzung für die Installation zusätzlicher Server ist ein installierter und laufender Administrationsserver, der vom aktuellen Rechner aus erreichbar ist.
- Wenn Sie Server zu einem WCM-System hinzufügen, das über einen Proxy-Admin-Server verwaltet wird (Proxy-System), muss nach der Installation ein Abgleich der Konfiguration von Master- und Proxy-System stattfinden.

Während der Installation neuer Server im Proxy-System dürfen im Master-System keine Konfigurationsänderungen vorgenommen werden. Ansonsten kommt es beim automatischen Übertragen von Konfigurationsänderungen durch den Master-Admin-Server zum Überschreiben der Einstellungen der neuen Server im Proxy-System. Um zu gewährleisten, dass keine Konfigurationsänderungen von anderen Benutzern vorgenommen werden, können Sie die Server in den Runlevel 4 “Einzelnutzer-Betrieb” setzen.

Informationen zum Abgleich der Konfiguration erhalten Sie im Livelink WCM Server-Administratorhandbuch (Kapitel “Server verwalten”).

- Wenn Sie mehrere in der JSP-Engine laufende Content-Server auf demselben Rechner einrichten, müssen unterschiedliche JSP-Engines zum Ausführen der Server verwendet werden. Passen Sie in diesem Fall nach der Installation von Livelink WCM Server in den Skripten zum Starten dieser Server die eingerichtete Standard-URL entsprechend der Konfiguration der verwendeten JSP-Engine an (siehe Abschnitt “Content-Server im Application-Server starten” auf Seite 170).
- Lucene-Suchserver können nur im gleichen Verzeichnis installiert werden, in dem der zugeordnete Server installiert ist.
- Beachten Sie außerdem die Informationen im Abschnitt “Hinweise zur Installation” auf Seite 72.

Vorgehensweise

Das Hinzufügen neuer Server zu einem bestehenden WCM-System erfolgt mithilfe des Installationsprogramms. Wenn Sie die bzw. den neuen Server auf einem anderen Rechner installieren möchten, müssen die entsprechenden Installationsdateien auf diesem Rechner verfügbar sein.

So installieren Sie nachträglich neue Server:

1. Starten Sie das Installationsprogramm, und wählen Sie das für die Installation vorgesehene Verzeichnis aus.

   Hinweis: Wenn für das WCM-System bereits ein Service-Pack installiert wurde, muss der Installationsaufruf angepasst werden (siehe Abschnitt “Installationsaufruf für ein WCM-System mit Service-Pack” auf Seite 121).

2. Aktivieren Sie im Dialog *Typ der Installation* das Optionsfeld *Server hinzufügen* (siehe Abschnitt “Typ der Installation auswählen” auf Seite 75), und klicken Sie auf die Schaltfläche *Weiter*.

3. Geben Sie im Dialog *Admin-Server* die Parameter des zuständigen Admin-Servers an, damit eine Verbindung zu diesem Server aufgebaut werden kann.

   Sie können diese Parameter im Admin-Client über *Konfiguration* → *Pools* → *WCM* → *{Pool des Admin-Servers}* überprüfen.

4. Klicken Sie auf die Schaltfläche *Testen*.

5. Sie müssen sich nun beim Admin-Server anmelden. Geben Sie die Benutzerkennung und das Passwort des zuständigen Administrators ein.

6. Bestätigen Sie den Dialog *Admin-Server* durch Klicken auf die Schaltfläche *Weiter*.

7. Der nächste Dialog bietet Ihnen automatisch die Option *Benutzerdefinierte Installation* an. Klicken Sie auf die Schaltfläche *Weiter*.

   Der Dialog *Server* wird geöffnet, in dem Sie die Angaben des neuen Servers eintragen können.

> **Hinweis:** Es werden Ihnen keine Register zur Installation bestimmter Komponenten angeboten. Installieren Sie die neuen Server mithilfe der Schaltfläche *Server hinzufügen*.

Detaillierte Informationen zu den einzelnen Parametern erhalten Sie im Abschnitt “Server einrichten” auf Seite 97.

8. Um weitere Server hinzuzufügen, klicken Sie auf die Schaltfläche *Server hinzufügen*. Es öffnet sich ein neues Register, auf dem Sie die erforderlichen Parameter eingeben können.

   Wenn Sie die Einträge für einen Server wieder entfernen möchten, gehen Sie auf das entsprechende Register, und klicken Sie auf die Schaltfläche *Server entfernen*.

9. Bestätigen Sie die Einstellungen durch Klicken auf die Schaltfläche *Weiter*.

   Die weiteren Schritte entsprechen der Minimalinstallation eines WCM-Systems.

Die Angaben im Startskript **startvip.bat** bzw. **startvip.sh** werden nach dem Hinzufügen einzelner Server automatisch angepasst, sodass die neuen Server mithilfe dieses Skripts gestartet werden können (siehe Abschnitt “Server starten” auf Seite 163.

Installationsaufruf für ein WCM-System mit Service-Pack

Um ein bestehendes WCM-System, für das bereits ein Service-Pack installiert wurde, zu erweitern, muss der Installationsaufruf entsprechend angepasst werden. Gehen Sie dazu wie folgt vor:

1. Kopieren Sie die Dateien **vipcore.jar**, **vipacs.jar** und **vipapi.jar** aus dem Verzeichnis **{WCM-Installationsverzeichnis}\lib** in ein lokales Verzeichnis.
2. Starten Sie die Installation mit folgendem Befehl:

Windows

```
install.bat {SDK-Installationsverzeichnis}\bin {Pfad zur Datei
   defaults.xml inklusive Dateiname} -INSTALLCLASSPATH {Pfad zum
   Verzeichnis aus Schritt 1}
```

UNIX

```
sh ./install.sh -jdk {SDK-Installationsverzeichnis}/bin
   -defaults {Pfad zur Datei defaults.xml inklusive Dateiname}
   -INSTALLCLASSPATH {Pfad zum Verzeichnis aus Schritt 1}
```

4.4 Admin-Client installieren

Das Installationsprogramm bietet Ihnen die Möglichkeit, den Admin-Client auf einem Rechner zu installieren, auf dem sich kein WCM-System befindet.

Hinweise

- Voraussetzung für die Installation eines weiteren Admin-Clients ist ein installierter und laufender Administrationsserver, der vom aktuellen Rechner aus erreichbar ist.
- Beachten Sie auch die Informationen im Abschnitt “Hinweise zur Installation” auf Seite 72.
- Wenn für das WCM-System bereits ein Service-Pack installiert wurde, muss der Installationsaufruf angepasst werden (siehe Abschnitt “Installationsaufruf für ein WCM-System mit Service-Pack” auf Seite 121).

- Sie können den Admin-Client auch nutzen, ohne ihn lokal zu installieren. Dazu erzeugen Sie für den Admin-Client eine Webanwendung und binden diese in einen Application-Server ein. Weitere Informationen hierzu finden Sie im Livelink WCM Server-Administratorhandbuch.

Vorgehensweise

So installieren Sie einen weiteren Admin-Client:

1. Starten Sie das Installationsprogramm, und wählen Sie das für die Installation vorgesehene Verzeichnis aus.
2. Aktivieren Sie im Dialog *Typ der Installation* das Optionsfeld *Admin-Client* (siehe Abschnitt "Typ der Installation auswählen" auf Seite 75), und klicken Sie auf die Schaltfläche *Weiter*.
3. Geben Sie im Dialog *Admin-Server* die Parameter des zuständigen Admin-Servers an, damit eine Verbindung zu diesem Server aufgebaut werden kann.

   Sie können diese Parameter im Admin-Client über *Konfiguration* → *Pools* → *WCM* → *{Pool des Admin-Servers}* überprüfen.
4. Klicken Sie auf die Schaltfläche *Testen*.
5. Sie müssen sich nun beim Admin-Server anmelden. Geben Sie die Benutzerkennung und das Passwort des zuständigen Administrators ein.
6. Bestätigen Sie den Dialog *Admin-Server* durch Klicken auf die Schaltfläche *Weiter*.
7. Klicken Sie auf die Schaltfläche *Fertig*.
8. Um den Admin-Client zu starten, rufen Sie die Datei **adminClient.bat** bzw. **adminClient.sh** im Verzeichnis **{WCM-Installationsverzeichnis}\admin** auf.

4.5 Lizenz erneuern

Hinweise

- Voraussetzung für das Erneuern der Lizenz ist ein installierter und laufender Administrationsserver, der vom aktuellen Rechner aus erreichbar ist.
- Beachten Sie auch die Informationen im Abschnitt “Hinweise zur Installation” auf Seite 72.
- Wenn für das WCM-System bereits ein Service-Pack installiert wurde, muss der Installationsaufruf angepasst werden (siehe Abschnitt “Installationsaufruf für ein WCM-System mit Service-Pack” auf Seite 121).

Vorgehensweise

Das Erneuern der Lizenz kann über einen beliebigen Rechner vorgenommen werden. So erneuern Sie die Lizenz:

1. Starten Sie das Installationsprogramm, und wählen Sie das für die Installation vorgesehene Verzeichnis aus.
2. Aktivieren Sie im Dialog *Typ der Installation* das Optionsfeld *Lizenz erneuern* (siehe Abschnitt “Typ der Installation auswählen” auf Seite 75), und klicken Sie auf die Schaltfläche *Weiter*.

   Sie werden aufgefordert, die Lizenzdatei auszuwählen.
3. Im Dialog *Lizenzdatei* können Sie nun den Pfad zur neuen Lizenzdatei angeben.

Hinweise:

Die Einstellungen für die Lizenzablaufbenachrichtigung können Sie im Admin-Client über *Konfiguration* → *Dienstprogramme* → *Lizenzablaufbenachrichtigung* ändern.

Den Zustand Ihrer WCM-Lizenzen können Sie jederzeit über *Systemverwaltung* → *Lizenzen* überprüfen.

Das Installationsprogramm überprüft die Lizenzdatei automatisch auf ihre Gültigkeit.

4. Klicken Sie auf die Schaltfläche *Weiter*.
5. Geben Sie im Dialog *Admin-Server* die Parameter des zuständigen Admin-Servers an, damit eine Verbindung zu diesem Server aufgebaut werden kann.

   Sie können diese Parameter im Admin-Client über *Konfiguration* → *Pools* → *WCM* → *{Pool des Admin-Servers}* überprüfen.
6. Klicken Sie auf die Schaltfläche *Testen*.
7. Sie müssen sich nun beim Admin-Server anmelden. Geben Sie die Benutzerkennung und das Passwort des zuständigen Administrators ein.
8. Bestätigen Sie den Dialog *Admin-Server* durch Klicken auf die Schaltfläche *Weiter*.
9. Klicken Sie auf die Schaltfläche *Fertig*.

4.6 Verzeichnisstruktur nach der Installation

Das Installationsprogramm legt im WCM-Installationsverzeichnis eine Reihe von Verzeichnissen für die verschiedenen Komponenten von Livelink WCM Server an.

Schreibrechte für die Verzeichnisse von Livelink WCM Server

Stellen Sie sicher, dass die Prozesse von Livelink WCM Server über die benötigten Rechte im Dateisystem verfügen. Der Benutzer, der die Installation des WCM-Systems durchführt, benötigt volle Schreibrechte für das WCM-Installationsverzeichnis.

Auch im laufenden Betrieb werden Dateien geändert, angelegt und gelöscht, sodass ein schreibender Zugriff auf folgende Unterverzeichnisse bzw. Dateien im WCM-Installationsverzeichnis erforderlich ist:

- für die Server bzw. JSP-Engine: **\temp**, **\log**, **\website**, **\fet**
- für das Portal Manager API im Zusammenhang mit dem Content-Client (Classic): **\data**
- für Suchserver: **\contentminer**

  Falls der Suchserver einem in der JSP-Engine laufenden Content-Server zugeordnet wurde, benötigt auch der Prozess der JSP-Engine Schreibrechte in diesem Verzeichnis.
- für das Schreiben von Trace-Protokollen: **\trace**
- für den Admin-Server: **\config**
- für das Setzen des Einmalpassworts in den Stoppskripten der Server (siehe Abschnitt “Server stoppen” auf Seite 169): **shutdown_{Servername}.bat** bzw. **.sh**

Im Folgenden werden die wichtigsten Verzeichnisse und Dateien im WCM-Installationsverzeichnis kurz erläutert.

Livelink WCM Server

Folgende Verzeichnisse und Dateien sind von Bedeutung:

- Startskripte für die Server: **startvip.bat** (bzw. **.sh**), **{Servername}.bat** (bzw. **.sh**) und **startserver.bat** (bzw. **.sh**)
- Skriptdatei zum Setzen des Klassenpfades: **setClasspath.bat** (bzw. **.sh**). Diese Datei wird im Rahmen der Startskripte automatisch aufgerufen.
- Skripte zum Herunterfahren der Server: **shutdown_{Servername}.bat** (bzw. **.sh**)

  Hinweis: Informationen zum Starten und Stoppen der Server sowie zum Aufbau der Startskripte erhalten Sie im Abschnitt 4.9 “Server starten und stoppen” ab Seite 162.

- Readme-Dateien zu Livelink WCM Server

Außerdem enthält das Installationsverzeichnis eine Reihe von Unterverzeichnissen:

- **\admin\:** enthält die Dateien des Admin-Clients und die Dateien des Export/Import-Tools
- **\config**: enthält die Konfigurationsdateien des WCM-Systems

  Achtung! An diesen Dateien dürfen **keinerlei** manuelle Änderungen vorgenommen werden, da das WCM-System ansonsten nicht mehr verwendet werden kann.

- **\documentation**: enthält die Dokumentation zu Livelink WCM Server im PDF-Format und die Javadoc zu den Programmierschnittstellen von Livelink WCM Server
- **\examples**: enthält Beispiele, u. a. für die Programmierung von Server-Agenten mithilfe des WCM Java API

- **\external_lib**: Verzeichnis für externe Bibliotheken, die in Livelink WCM Server eingebunden werden (u.a. JDBC-Treiber)
- **\fet**: enthält wichtige Dateien für das Deployment
- **\installation**: enthält die Protokolldateien, die während der Installation angelegt werden. Im Unterverzeichnis **\service** befinden sich Dateien zum Einrichten der Server als Dienst.
- **\keys**: enthält die Serverzertifikate des WCM-Truststores
- **\latestpatch**: Verzeichnis für die Service-Pack-Dateien **vipacs.jar**, **vipapi.jar** und **vipcore.jar**
- **\lib**: enthält die von Livelink WCM Server verwendeten Klassenarchive
- **\log**: enthält die Protokoll- und Fehlerdateien der Server (siehe Abschnitt 4.10 “Protokoll- und Fehlerdateien” auf Seite 174) und des Export/Import-Tools
- **\tools**: enthält die Skriptdatei **precompile.bat** (bzw. **.sh**) zum Vorkompilieren des Content-Clients (siehe Abschnitt “Das Precompile-Skript” auf Seite 202). Außerdem befindet sich in diesem Verzeichnis das Skript **setPomaClasspath.bat** (bzw. **.sh**) zum expliziten Setzen des Klassenpfads. Dieses Skript wird benötigt, wenn der Content-Server in einer JSP-Engine ohne eigenen Class-Loader läuft.
- **\VIPSecure**: enthält die Dateien für die Zugriffssteuerungskomponente Secure Access
- **\website**: Standard-Verzeichnis zum Speichern von Website-Daten. Im Unterverzeichnis **\cmsclient** befinden sich die Dateien des Content-Clients. Im Unterverzeichnis **\htmlclient** befinden sich die Dateien des Content-Clients (Classic).

Suchserver

Content Miner-Suchserver

Folgende Verzeichnisse sind für Content Miner-Suchserver von Bedeutung:

- **\contentminer\{Name des Suchservers}\server**: enthält die Startskripte für die Content Miner-Suchserver (siehe Abschnitt “Suchserver starten” auf Seite 172)
- **\contentminer\{Name des Suchservers}\tools**: enthält die vorkonfigurierten Kommandozeilen-Tools

Lucene-Suchserver

Folgende Verzeichnisse sind für Lucene-Suchserver von Bedeutung:

- **\contentminer\{Name des Suchservers}\index**: enthält den Index
- **\contentminer\{Name des Suchservers}\tools**: enthält die vorkonfigurierten Kommandozeilen-Tools

Livelink-Suchserver

Folgendes Verzeichnis ist für Livelink-Suchserver von Bedeutung:

\livelinksearch\{Name des Suchservers}\tools: enthält die vorkonfigurierten Kommandozeilen-Tools

Beispiele für den Einsatz von Suchservern

Im Verzeichnis **\examples\SearchServer** finden Sie einfache Beispiele für den Einsatz von Suchservern. Um diese Dateien verwenden zu können, müssen Sie den HTTP-Server und die JSP-Engine entsprechend konfigurieren.

Des Weiteren können die Dateien mithilfe der im Verzeichnis **\examples** mitgelieferten Datei **multiimport.zip** in eine bestehende Website importiert werden. Die Startdatei für den Import heißt **index.htm**. Informationen zum Import aus einer ZIP-Datei finden Sie im Content-Client-Benutzerhandbuch.

Tag Libraries

Zur besseren Strukturierung von JSP-Seiten stellt die JSP-Spezifikation in der Version 1.1 so genannte *Tag Libraries* (kurz Taglibs) zur Verfügung.

Zum Lieferumfang von Livelink WCM Server gehören einige Tag Libraries, die sich im Verzeichnis **{WCM-Installationsverzeichnis}\examples\taglets** befinden. Informationen zu Programmierbeispielen erhalten Sie in der mitgelieferten Online-Dokumentation (**ReadMe.html**). Weitere Informationen zu Taglets finden Sie im Content Miner-Handbuch.

4.7 WCM-System deinstallieren

Mithilfe des Installationsprogramms können Sie ein komplettes WCM-System bzw. einzelne Komponenten des Systems deinstallieren.

Bei einer erfolgreichen Deinstallation werden alle entsprechenden Dateien, Verzeichnisse und Registry-Einträge vom Installationsprogramm automatisch entfernt.

Das Installationsprogramm löscht jedoch nicht die von den WCM-Komponenten angelegten und genutzten Datenbanktabellen. Dies müssen Sie nach einer Deinstallation des kompletten WCM-Systems manuell tun (siehe Abschnitt “Datenbanktabellen löschen” auf Seite 134).

Die Deinstallation von Komponenten kann auf zwei Wegen erfolgen:

- mithilfe des WCM-Installationsprogramms, siehe folgenden Abschnitt
- mithilfe der Konsole, siehe Abschnitt 4.8 “Installation und Deinstallation über die Konsole steuern” auf Seite 135

Hinweise zur Deinstallation

- Voraussetzung für die Deinstallation eines WCM-Systems ist ein installierter und laufender Administrationsserver, der vom aktuellen Rechner aus erreichbar sein muss.
- Das Verzeichnis, in dem Sie die Deinstallation vornehmen möchten, muss Komponenten eines WCM-Systems enthalten. Andernfalls ist die Option *Deinstallation* nicht aktiviert.
- Ein Server kann nur dann deinstalliert werden, wenn ihm keine Websites mehr zugeordnet sind. Löschen Sie die entsprechenden Websites gegebenenfalls vor der Deinstallation über den Admin-Client, oder ordnen Sie sie einem anderen Server zu.

  Ist dies nicht mehr möglich, z.B. weil der entsprechende Server beschädigt oder aus anderen Gründen nicht mehr erreichbar ist, kann der Server nicht über das Installationsprogramm entfernt werden. Benutzen Sie in einem solchen Fall die Funktion *Server löschen* in der Ansicht *Konfiguration* des Admin-Clients (siehe Livelink WCM Server-Administratorhandbuch)
- Ist einem Server, den Sie entfernen möchten, ein Suchserver zugeordnet, der sich im selben Verzeichnis wie der Server befindet, dann wird der entsprechende Suchserver automatisch ebenfalls deinstalliert. Befindet sich der Suchserver in einem anderen Verzeichnis als der Server, dann muss er separat über den Deinstallationsvorgang entfernt werden.
- Beim Entfernen einzelner Server werden die Angaben im Startskript **startvip.bat** bzw. **startvip.sh** automatisch angepasst.

Komponenten über die grafische Oberfläche deinstallieren

So deinstallieren Sie Komponenten über die grafische Oberfläche:

1. Starten Sie das Installationsprogramm, und wählen Sie das Installationsverzeichnis aus.
2. Aktivieren Sie im Dialog *Typ der Installation* das Optionsfeld *Deinstallation* (siehe Abschnitt “Typ der Installation auswählen” auf Seite 75), und klicken Sie auf die Schaltfläche *Weiter*.
3. Geben Sie im Dialog *Admin-Server* die Parameter des zuständigen Admin-Servers an, damit eine Verbindung zu diesem Server aufgebaut werden kann.

   Sie können diese Parameter im Admin-Client über *Konfiguration* → *Pools* → *WCM* → *{Pool des Admin-Servers}* überprüfen.
4. Klicken Sie auf die Schaltfläche *Testen*.
5. Sie müssen sich nun beim Admin-Server anmelden. Geben Sie die Benutzerkennung und das Passwort des zuständigen Administrators ein.
6. Bestätigen Sie den Dialog *Admin-Server* durch Klicken auf die Schaltfläche *Weiter*.

   Im nächsten Dialog werden die Komponenten Ihres WCM-Systems angezeigt, die deinstalliert werden können. Wenn die Server, die Sie entfernen möchten, inaktiv dargestellt sind, sind ihnen möglicherweise noch Websites zugeordnet.

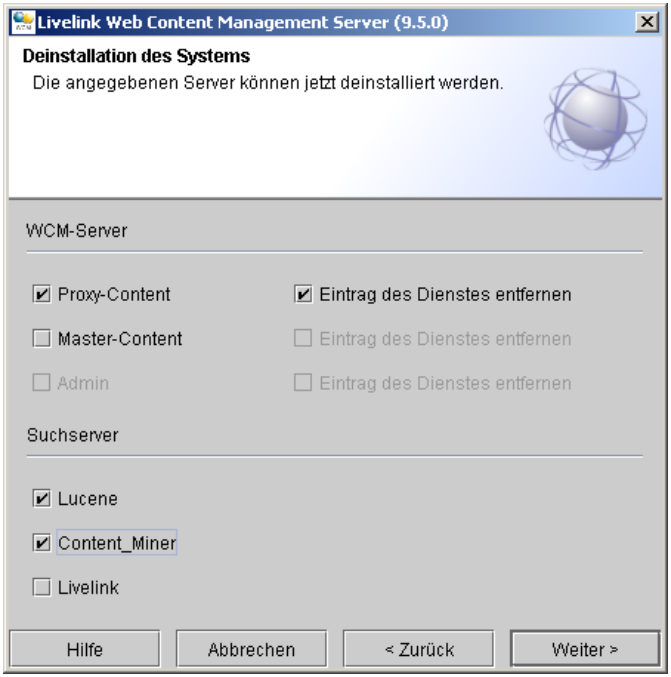


Abb. 19 – Auswahl der zu entfernenden Komponenten

7. Aktivieren Sie die Kontrollkästchen der Komponenten, die aus dem WCM-System entfernt werden sollen.

   Für Server können Sie zusätzlich das Kontrollkästchen *Eintrag des Dienstes entfernen* aktivieren. Damit wird der Eintrag zum automatischen Starten des Servers aus der Windows-Registrierung entfernt.

   Hinweis: Mithilfe der Skripte **uninstall_{Servername}.bat** im Verzeichnis **{WCM-Installationsverzeichnis}\installation\service** können Sie unabhängig von der Server-Deinstallation die Dienste aus der Windows-Registrierung entfernen.

8. Klicken Sie auf die Schaltfläche *Weiter*.

Im letzten Dialog des Installationsassistenten werden die zu deinstallierenden Komponenten zusammenfassend angezeigt.

9. Klicken Sie auf die Schaltfläche *Fertig*.

Datenbanktabellen löschen

Wenn Sie das WCM-System vollständig entfernt haben, müssen nach der Deinstallation die von Livelink WCM Server genutzten Tabellen in der Datenbank gelöscht werden. Die folgende Beschreibung bezieht sich auf das RDBMS Oracle.

Löschen Sie folgende Tabellen in der Oracle-Datenbank. Sie können dazu den SQL-Befehl `drop table {Name}` verwenden.

- ADMIN_FIELDINFO
- ADMIN_FUNCAREA_GROUP
- ADMIN_FUNCAREA_ROLE
- ADMIN_FUNCAREA_USER
- ADMIN_GROUP
- ADMIN_HCL
- ADMIN_ROLE
- ADMIN_SUBST_USER
- ADMIN_USER
- ADMIN_USER_GROUP
- ADMIN_USER_ROLE
- ADMIN_VIP_VER

- ADMIN_WEBSITE_GROUP
- ADMIN_WEBSITE_ROLE
- ADMIN_WEBSITE_USER

4.8 Installation und Deinstallation über die Konsole steuern

Alternativ zur Installation über die grafische Oberfläche können das WCM-System und einzelne Komponenten auch mithilfe der Konsole installiert und deinstalliert werden.

Hinweis: Die Konsoleninstallation führt weniger Prüfungen auf Korrektheit der über die Datei **defaults.xml** gemachten Angaben durch als die Installation über die grafische Oberfläche. Dies lässt Ihnen mehr Freiheiten bei der Installation, kann jedoch auch leichter zu Problemen führen.

Parameter in der Datei `defaults.xml`

Die erforderlichen Parameter für die Installation und Deinstallation werden standardmäßig aus der Datei **defaults.xml** gelesen, die sich im Verzeichnis **\installation** auf der WCM-CD befindet. Diese Datei enthält sämtliche Standardeinstellungen, die bei der Installation bzw. Deinstallation verwendet werden. Kopieren Sie die Datei auf ein lokales Laufwerk, und passen Sie die Einträge entsprechend Ihren Vorgaben an.

Die Datei **defaults.xml** ist in mehrere Abschnitte für die verschiedenen Komponenten von Livelink WCM Server unterteilt. Mithilfe des Parameters `<install_action>` können Sie für jede Komponente individuell festlegen, ob die entsprechende Komponente installiert, deinstalliert oder durch das Installationsprogramm nicht verändert werden soll.

Hinweis: Der Parameter `<install_action>` im Abschnitt `<common>` steuert die Installationsoption für das Basissystem. Tragen Sie hier `install` ein, wenn das gesamte WCM-System oder eine einzelne Komponente installiert wird. `uninstall` sollte hier nur eingetragen werden, wenn das **gesamte** WCM-System entfernt werden soll.

Installation und Deinstallation werden über verschiedene Skripte gesteuert (siehe Abschnitt “Installation über die Konsole starten” auf Seite 160 und Abschnitt “Deinstallation über die Konsole starten” auf Seite 161.

Das folgende Beispiel stellt die erforderlichen Einstellungen für die Installation eines Master-Admin-Servers mit RDBMS-Datenhaltung und eines Master-Content-Servers, der als Webanwendung in einem Application-Server ausgeführt wird, dar. Dieses Szenario entspricht einer Minimalinstallation.

Hinweis: Der Installationsvorgang wird abgebrochen, wenn der WCM-Administrator nicht erfolgreich angelegt werden konnte oder wenn der Administrationsserver nicht gestartet oder erreicht werden konnte.

```
<default>

      <license>
         <directory>license.xml</directory>
         <mailto>wcmadmin@company.example</mailto>
         <daysbefore>10</daysbefore>
         <percentage>80</percentage>
      </license>

      <common>
         <language>de_DE</language>
         <directory>d:\wcm</directory>
         <directory_unix>/export/home/wcmuser/wcmsystem/wcm
            </directory_unix>
         <vipadminuser>admin</vipadminuser>
         <vipadminpassword>admin</vipadminpassword>
         <default_suffix>htm</default_suffix>
         <server_languages>en_US de_DE</server_languages>
```

```
   <install_action>install</install_action>
</common>

<admin>
   <name>Admin</name>
   <server_category>master</server_category>
   <host>wcmserver.company.example</host>
   <http_port>5003</http_port>
   <vipp_port>5002</vipp_port>
   <secure>false</secure
   <storage>rdbms</storage>
   <mailhost>mailserver.company.example</mailhost>
   <mailsender>wcm@company.example</mailsender>
   <nt_service>false</nt_service>
   <install_action>install</install_action>
</admin>

<server name="Master-Content">
   <server_type>content</server_type>
   <server_category>master</server_category>
   <host>wcmserver.company.example</host>
   <http_port>5005</http_port>
   <vipp_port>5004</vipp_port>
   <secure>false</secure>
   <encoding>UTF-8</encoding>
   <nt_service>false</nt_service>
   <create_application_file>true</create_application_file>
   <application_file_dir>d:\temp</application_file_dir>
   <application_name>wcm</application_name>
   <application_with_client>true</application_with_client>
   <application_client_name>cmsclient</application_client_name>
   <application_file_template>web23.xml
      </application_file_template>
   <application_servlet></application_servlet>
   <application_taglet></application_taglet>
   <application_filter></application_filter>
   <application_encoding>UTF-8</application_encoding>
   <application_default>false</application_default>
   <install_action>install</install_action>
</server>

<rdbms>
   <poolname>userpool</poolname>
   <user>wcmuser</user>
   <password>wcm</password>
   <type>ORACLE</type>
   <db_owner></db_owner>
   <jdbc_driver>oracle.jdbc.driver.OracleDriver</jdbc_driver>
   <driverclasspath></driverclasspath>
```

```
        <connection_string>
           jdbc:oracle:thin:@dbserver.company.example:1521:wcmdb
        </connection_string>
        <check>true</check>
      </rdbms>

</default>
```

Die Datei **defaults.xml** ist in mehrere Hauptabschnitte unterteilt:

- <license> </license>, siehe Abschnitt “Angaben im Abschnitt <license>” auf Seite 139
- <common> </common>, siehe Abschnitt “Angaben im Abschnitt <common>” auf Seite 140
- <admin> </admin>, siehe Abschnitt “Angaben im Abschnitt <admin>” auf Seite 142
- <update_vip> </update_vip>, siehe Abschnitt “Angaben im Abschnitt <update_vip>” auf Seite 237
- <update_rdbms> </update_rdbms>, siehe Abschnitt “Angaben im Abschnitt <update_rdbms>” auf Seite 239
- <server> </server>, siehe Abschnitt “Angaben im Abschnitt <server>” auf Seite 144
- <contentminer_server> </contentminer_server>, siehe Abschnitt “Angaben im Abschnitt <contentminer_server>” auf Seite 148
- <lucene_server> </lucene_server>, siehe Abschnitt “Angaben im Abschnitt <lucene_server>” auf Seite 149
- <livelink_search-server> </livelink_search-server>, siehe Abschnitt “Angaben im Abschnitt <livelink_search-server>” auf Seite 150
- <external_libs> </external_libs>, siehe Abschnitt “Angaben im Abschnitt <external_libs>” auf Seite 152

- <rdbms> </rdbms>, siehe Abschnitt “Angaben im Abschnitt <rdbms>” auf Seite 152
- <livelink> </livelink>, siehe Abschnitt “Angaben im Abschnitt <livelink>” auf Seite 155
- <ldap> </ldap>, siehe Abschnitt “Angaben im Abschnitt <ldap>” auf Seite 157
- <converter> </converter>: Angaben für LDAP-Verzeichnisdienste, u.a. Mapping von LDAP-Attributen auf WCM-Attribute (siehe Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45)

Die folgenden Abschnitte erläutern die einzelnen Angaben.

Angaben im Abschnitt <license>

Dieser Abschnitt enthält die Angaben zur Lizenzdatei und einige Parameter der Lizenzverwaltung.

> **Hinweis:** Beachten Sie auch die Informationen zu diesen Parametern im Abschnitt “Optionen für die Lizenzverwaltung festlegen” auf Seite 77.

Tabelle 9 – Angaben im Abschnitt <license>

Eintrag in der XML-Datei	Erläuterung
<directory>license.xml</directory>	Vollständiger Pfad zur Lizenzdatei
<mailto>wcmadmin@company.example</mailto>	E-Mail-Adresse des Verantwortlichen, der bei Ablauf oder Überschreitung der WCM-Lizenzen benachrichtigt werden soll

Eintrag in der XML-Datei	Erläuterung
<daysbefore>10</daysbefore>	Option für das Senden der Lizenzablaufbenachrichtigung: Anzahl der Tage vor Ablauf der Lizenzen
<percentage>80</percentage>	Option für das Senden der Lizenzablaufbenachrichtigung: Prozentsatz der ausgelasteten Lizenzen für aktive Benutzer

Angaben im Abschnitt <common>

Dieser Abschnitt enthält allgemeine Parameter der Installation wie Sprache und Verzeichnis, Informationen zum WCM-Administrator sowie die Installationsoption für das Basissystem.

Tabelle 10 – Angaben im Abschnitt <common>

Eintrag in der XML-Datei	Erläuterung
<language>de_DE</language>	Die Sprache der Installationsdialoge und die initiale Sprache des Administrators Mögliche Werte: Spracheinstellungen im Format Sprachcode_Ländercode entsprechend ISO-639 und ISO-3166
<directory>d:\wcm</directory>	Zielverzeichnis unter Windows, in das das WCM-System installiert werden soll
<directory_unix>/home/wcmuser/wcmsystem/wcm</directory_unix>	Zielverzeichnis unter UNIX, in das das WCM-System installiert werden soll

Eintrag in der XML-Datei	Erläuterung
`<vipadminuser>admin</vipadminuser>`	Benutzerkennung des WCM-Administrators Siehe Abschnitt “WCM-Administrator einrichten” auf Seite 93
`<vipadminpassword>admin</vipadminpassword>`	Passwort des WCM-Administrators
`<default_suffix>htm</default_suffix>`	Standard-Dateinamenerweiterung für generierte Seiten Siehe Abschnitt “Parameter des neuen Administrationsservers einstellen” auf Seite 79
`<server_languages>en_US de_DE</server_languages>`	Die Basissprache(n) der Server Mögliche Werte: Spracheinstellungen im Format `Sprachcode_Ländercode` entsprechend ISO-639 und ISO-3166
`<install_action>install</install_action>`	Installationsoption für das Basissystem Mögliche Werte: `install` (beim Hinzufügen von Komponenten zum WCM-System), `uninstall` (nur bei Deinstallation des gesamten WCM-Systems), `none` (keine Veränderung, z.B. beim Entfernen einzelner Komponenten aus einem bestehenden WCM-System oder beim Upgrade des WCM-Systems) Informationen zum Basissystem enthält auch der Abschnitt “Zusammenfassung der Komponenten” auf Seite 113.

Angaben im Abschnitt <admin>

Dieser Abschnitt enthält die Angaben des Administrationsservers.

> **Hinweis:** Beachten Sie auch die Informationen zu den einzelnen Parametern im Abschnitt “Parameter des neuen Administrationsservers einstellen” auf Seite 79.

Tabelle 11 – Angaben im Abschnitt <admin>

Eintrag in der XML-Datei	Erläuterung
<name>Admin</name>	Name des Administrationsservers
<server_category>master</server_category>	Serverkategorie des Administrationsservers Mögliche Werte: master und proxy
<host>wcmserver.company.example</host>	Voll qualifizierter Hostname des Rechners, auf dem der Administrationsserver installiert werden soll
<http_port>5003</http_port>	Port des Admin-Servers für die HTTP-Verbindung (HTTP-Tunneling)
<vipp_port>5002</vipp_port>	Port des Admin-Servers für die VIPP-Verbindung
<secure>false</secure>	Angabe, ob die Kommunikation zwischen den Servern über gesicherte Verbindungen (Secure Socket Layer) erfolgen soll Mögliche Werte: true oder false

Eintrag in der XML-Datei	Erläuterung
`<storage>rdbms</storage>`	Art der Speicherung der Benutzerdaten Mögliche Werte: `rdbms`, `ldap` oder `livelink`
`<mailhost>mailserver.company.example</mailhost>`	Voll qualifizierter Hostname des SMTP-Servers
`<mailsender>wcm@company.example</mailsender>`	Mailadresse, die als Absender für E-Mails verwendet wird, die das System verschickt
`<nt_service>false</nt_service>`	Angabe, ob der Administrationsserver als Windows-Dienst eingerichtet werden soll. Mit diesem Dienst lässt sich der Server unter Windows automatisch starten und beenden. Mögliche Werte: `true` oder `false`
`<install_action>install</install_action>`	Installationsoption für den Administrationsserver Mögliche Werte: `install` (Installation), `uninstall` (Deinstallation), `none` (keine Veränderung, z. B. beim Hinzufügen von Servern zu einem bestehenden WCM-System oder beim Upgrade des WCM-Systems) Wenn Sie `none` eintragen, wird vom Installationsprogramm automatisch die Verbindung zum Master-Admin-Server überprüft.

Angaben im Abschnitt <server>

Dieser Abschnitt enthält Angaben zu den Content-Servern, die installiert werden sollen. Für jeden Content-Server, der installiert werden soll, ist ein separater Absatz auszufüllen.

> **Hinweis:** Beachten Sie auch die Hinweise zu diesen Parametern im Abschnitt “Server einrichten” auf Seite 97.

Tabelle 12 – Angaben im Abschnitt <server>

Eintrag in der XML-Datei	Erläuterung
<server name="Master-Content">	Name des Content-Servers
<server_type>content</server_type>	Servertyp Der Wert ist immer content.
<server_category>master</server_category>	Serverkategorie Mögliche Werte: master und proxy
<host>wcmserver.company.example</host>	Voll qualifizierter Hostname des Rechners, auf dem der Content-Server installiert werden soll
<http_port>5005</http_port>	Port des Content-Servers für die HTTP-Verbindung (HTTP-Tunneling)
<vipp_port>5004</vipp_port>	Port des Content-Servers für die VIPP-Verbindung

Eintrag in der XML-Datei	Erläuterung
`<secure>false</secure>`	Angabe, ob die Kommunikation zwischen den Servern über gesicherte Verbindungen (Secure Socket Layer) erfolgen soll Mögliche Werte: `true` oder `false`
`<encoding>UTF-8</encoding>`	Nur für Content-Server verfügbar, die in der JSP-Engine laufen Encoding für den Content-Client Mögliche Werte: `UTF-8` (Unicode), `ISO-8859-1` (Latin-1)
`<nt_service>false</nt_service>`	Nicht für Content-Server verfügbar, die in der JSP-Engine laufen Angabe, ob dieser Server als Window-Dienst eingerichtet werden soll. Mit diesem Dienst lässt sich der Server unter Windows automatisch starten und beenden. Mögliche Werte: `true` oder `false`
`<create_application_file>false</create_application_file>`	Angabe, ob für diesen Server eine Webanwendung erzeugt werden soll. Um mit dem Content-Client bzw. dem Content-Client (Classic) arbeiten zu können, muss mindestens einer der Content-Server im Kontext einer JSP-Engine oder als Webanwendung in einem Application-Server ausgeführt werden. Mögliche Werte: `true` oder `false`
`<application_file_dir>d:\temp<application_file_dir>`	Verzeichnis, in dem die erzeugte WAR-Datei gespeichert werden soll

Eintrag in der XML-Datei	Erläuterung
`<application_name>wcm</application_name>`	Name für die erzeugte Webanwendung. Dieser Name bestimmt den Dateinamen der WAR-Datei und wird Bestandteil der URL, über die die Webanwendung im Application-Server aufgerufen wird.
`<application_with_client>true</application_with_client>`	Angabe, ob der Content-Client in die Webanwendung eingebunden wird Mögliche Werte: `true` oder `false`
`<application_client_name>cmsclient</application_client_name>`	Nur verfügbar, wenn der Eintrag `<application_with_client>` den Wert `true` hat Name für den Content-Client. Analog zum Namen der Webanwendung wird auch der Name des Content-Clients an die URL angefügt, über die der Content-Client aufgerufen wird.

`<application_file_template>web23.xml</application_file_template>`	Verwendeter Application-Server. Alternativ zu einem Produkt kann auch ein Servlet-API-Standard angegeben werden.
	Mögliche Werte:
	`servlet-api22.xml`
	`servlet-api23.xml`
	`websphere4.xml`
	`websphere5.xml`
	`weblogic81.xml`
	`tomcat4110.xml`
	`oracle9i.xml`
	`resin214.xml`
	`jrun4.xml`
	`servletexec42.xml`

Eintrag in der XML-Datei	Erläuterung

`<application_servlet></application_servlet>`
`<application_taglet></application_taglet>`
`<application_filter></application_filter>`
	Mapping von Servlets, Tag Libraries und Filter-Servlets, die nicht in Livelink WCM Server verwendet werden, aber in der erzeugten Webanwendung verfügbar sein sollen
	
	Hinweis: Bitte beachten Sie, dass in diesen Parametern valides XML eingegeben werden muss und die Zeichen < bzw. > durch `<` bzw. `>` codiert werden müssen (Beispiel: `<servlet>` wird zu `<servlet>`).

`<application_encoding>UTF-8</application_encoding>`	Encoding für die Webanwendung Mögliche Werte: `UTF-8` (Unicode), `ISO-8859-1` (Latin-1)
`<application_default>false</application_default>`	Angabe, ob die erzeugte Webanwendung im Application-Server als Standardanwendung (default application) definiert ist. Die Standardanwendung wird über die Root-URL des Application-Servers angesprochen, d.h., die URL enthält nicht den Anwendungsnamen. Mögliche Werte: `true` oder `false`
`<install_action>install</install_action>`	Installationsoption für den Server Mögliche Werte: `install` (Installation), `uninstall` (Deinstallation), `none` (keine Veränderung, z. B. beim Upgrade des WCM-Systems)

Angaben im Abschnitt <contentminer_server>

Dieser Abschnitt enthält Angaben zu den Content Miner-Suchservern.

> **Hinweis:** Beachten Sie auch die Informationen zu diesen Parametern im Abschnitt “Register Content Miner” auf Seite 105.

Tabelle 13 – Angaben im Abschnitt <contentminer_server>

Eintrag in der XML-Datei	Erläuterung
`<contentminer_server name="Contentminer1">`	Name des Content Miner-Suchservers
`<host>wcmserver.company.example</host>`	Voll qualifizierter Hostname des Rechners, auf dem der Content Miner-Suchserver installiert werden soll
`<query>9000</query>`	Port des Query-Servers für die Verbindung
`<index>9001</index>`	Port des Index-Servers für die Verbindung
`<vip_server>Master-Content</vip_server>`	Name eines vorhandenen bzw. zu installierenden Content-Servers, dem dieser Suchserver zugeordnet werden soll
`<install_action>install</install_action>`	Installationsoption für den Suchserver Mögliche Werte: `install` (Installation), `uninstall` (Deinstallation), `none` (keine Veränderung, z.B. beim Upgrade des WCM-Systems)

Angaben im Abschnitt <lucene_server>

Dieser Abschnitt enthält Angaben zu den Lucene-Suchservern.

> **Hinweis:** Beachten Sie auch die Informationen zu diesen Parametern im Abschnitt “Register Lucene” auf Seite 108.

Tabelle 14 – Angaben im Abschnitt <lucene_server>

Eintrag in der XML-Datei	Erläuterung
<lucene_server name="Lucene1">	Name des Lucene-Suchservers
<reload_interval>300000</reload_interval>	Zeitspanne in Millisekunden, nach der alle Collections für den lesenden Zugriff neu geladen werden
<vip_server>Master-Content</vip_server>	Name eines vorhandenen bzw. zu installierenden Content-Servers, dem dieser Suchserver zugeordnet werden soll

Eintrag in der XML-Datei	Erläuterung

`<index_location>`
`<server name="Master-Content">d:\temp</server>`
`</index_location>`
	Pfad zu dem Verzeichnis im Dateisystem, in dem der Index gespeichert ist. Dieser Speicherort muss von allen Servern erreichbar sein. Der Speicherort wird für jeden Server individuell eingestellt, wobei die Pfade für alle Server auf das gleiche Verzeichnis zeigen müssen.

`<install_action>install</install_action>`	Installationsoption für den Suchserver Mögliche Werte: `install` (Installation), `uninstall` (Deinstallation), `none` (keine Veränderung, z.B. beim Upgrade des WCM-Systems)

Angaben im Abschnitt <livelink_search-server>

Dieser Abschnitt enthält Angaben zu den Livelink-Suchservern.

Hinweis: Beachten Sie auch die Informationen zu diesen Parametern im Abschnitt “Register Livelink” auf Seite 110.

Tabelle 15 – Angaben im Abschnitt `<livelink_search-server>`

Eintrag in der XML-Datei	Erläuterung
`<livelink_search-server name="Livelink1">`	Name des Livelink-Suchservers
`<vip_server>Master-Content</vip_server>`	Name eines vorhandenen bzw. zu installierenden Content-Servers, dem dieser Suchserver zugeordnet werden soll

`<url>`
`http://livelink.company.example/livelink/livelink.exe`
`</url>`
	URL zum Livelink-Server, der die Indexierung durchführen und die Suchanfragen bearbeiten soll

`<host>livelink.company.example</host>`	Voll qualifizierter Hostname des Rechners, auf dem der Livelink-Server installiert ist, der die Indexierung durchführen und die Suchanfragen bearbeiten soll
`<port>2099</port>`	Port des Livelink-Servers für die Verbindung
`<urlusable>true</urlusable>`	Angabe, ob für die Verbindung zum Livelink-Server dessen URL verwendet werden soll. Die Einträge `<host>` und `<port>` werden in dem Fall ignoriert.
`<username>Admin</username>`	Benutzer für die Bearbeitung der Suchanfragen im Livelink-System. Der Benutzer muss lesend auf die Segmente (Collections) zugreifen können.

Eintrag in der XML-Datei	Erläuterung
`<password>admin</password>`	Passwort für die Bearbeitung der Suchanfragen im Livelink-System
`<install_action>install</install_action>`	Installationsoption für den Suchserver Mögliche Werte: `install` (Installation), `uninstall` (Deinstallation), `none` (keine Veränderung, z.B. beim Upgrade des WCM-Systems)

Angaben im Abschnitt <external_libs>

In diesem Abschnitt können Sie den Pfad zu externen Bibliotheken eintragen, die vom Installationsprogramm automatisch in das Verzeichnis **{WCM-Installationsverzeichnis}\external_lib** kopiert werden sollen. Mehrere Pfade werden durch Semikolon (Windows) bzw. Doppelpunkt (UNIX) getrennt.

Angaben im Abschnitt <rdbms>

Dieser Abschnitt enthält die Parameter für die Verbindung des Administrationsservers zum relationalen Datenbank-Managementsystem. Für jedes der unterstützten RDBMS enthält die Datei **defaults.xml** einen separaten Absatz mit den Standardvorgaben.

Hinweis: Beachten Sie auch die Informationen zu diesen Parametern im Abschnitt “Parameter des RDBMS einstellen” auf Seite 82.

Tabelle 16 – Angaben im Abschnitt `<rdbms>`

Eintrag in der XML-Datei	Erläuterung
`<poolname>userpool</poolname>`	Name des JDBC-Pools, der für die Verbindungen zum RDBMS angelegt wird
`<user>wcmuser</user>`	Benutzerkennung, die vom WCM-System für die Anmeldung bei der Datenbank verwendet wird
`<password>wcm</password>`	Passwort, das vom WCM-System für die Anmeldung bei der Datenbank verwendet wird
`<type>ORACLE</type>`	Typ des Datenbank-Managementsystems Mögliche Werte: `ORACLE`, `MS SQLServer2000`
`<db_owner></db_owner>`	Nur für SQL Server Eigentümer der Datenbank, d. h. Kennung des Benutzers, der die entsprechenden Tabellen angelegt hat
`<jdbc_driver>oracle.jdbc.driver.OracleDriver</jdbc_driver>`	Name der Treiberklasse für das verwendete RDBMS

Eintrag in der XML-Datei	Erläuterung
`<driverclasspath></driverclasspath>`	Absoluter Pfad zur Datei bzw. zu den Dateien mit den JDBC-Treibern für die verwendete Datenbank. Besteht der Treiber aus mehreren Dateien, geben Sie die Pfade getrennt durch ; (Semikolon) ein. Das Installationsprogramm kopiert die Datei(en) mit den JDBC-Treibern in das Verzeichnis **{WCM-Installationsverzeichnis}\external_lib**. Dies erfolgt auf allen Servern. Beispielwert: `msbase.jar;mssqlserver.jar;msutil.jar` (Microsoft-Treiber für MS SQL Server)

`<connection_string>`
`jdbc:oracle:thin:@dbserver.company.example:1521:wcmdb`
`</connection_string>`
	Vollständige Bezeichnung der Datenquelle. Dieser Parameter enthält den voll qualifizierten Hostnamen des Datenbank-Servers, den Port für die Verbindung zum Datenbank-Server und den Namen der Datenbank.

`<check>true</check>`	Angabe zur Überprüfung der Verbindung zwischen dem Master-Admin-Server und dem Datenbank-Managementsystem. Bei der Installation eines Proxy-Admin-Servers muss der Parameter auf `false` gesetzt werden. Mögliche Werte: `true` oder `false`

Angaben im Abschnitt <livelink>

Dieser Abschnitt enthält die Parameter für die Verbindung des Administrationsservers zur Livelink-Benutzerverwaltung.

> **Hinweis:** Beachten Sie auch die Informationen zu diesen Parametern im Abschnitt “Parameter des Livelink-Systems einstellen” auf Seite 86.

Tabelle 17 – Angaben im Abschnitt <livelink>

Eintrag in der XML-Datei	Erläuterung
<poolname>userpool</poolname>	Name des Livelink-Pools, der für die Verbindungen zum Livelink-System angelegt wird
<host>livelink.company.example</host>	Voll qualifizierter Hostname des Rechners, auf dem der Livelink-Server installiert ist
<port>2099</port>	Port-Nummer für die Verbindung zum Livelink-Server Dieser Wert entspricht dem Wert der Variable Port im Abschnitt [general] der Datei **opentext.ini** (Standardwert: 2099).
<user>Admin</user>	Benutzer für den Zugriff auf den Livelink-Server. Der Benutzer muss im Livelink-System Benutzer und Gruppen anlegen, ändern und löschen dürfen.
<password>admin</password>	Passwort für den Zugriff auf den Livelink-Server

Eintrag in der XML-Datei	Erläuterung
`<database></database>`	Logischer Name der verwendeten Livelink-Datenbank. Im Normalfall tragen Sie hier keinen Wert ein, d.h., es wird die Datenbank benutzt, die im Livelink-System als Standard konfiguriert ist.

`<secure>false</secure>`
`<https>true</https>`
`<livelinkcgi>/intranet/llisapi.dll</livelinkcgi>`
`<httpusername>Admin</httpusername>`
`<httppassword>password</httppassword>`
`<verifyserver>true</verifyserver>`
`<domainname />`
	Achtung! Diese Einträge dürfen nicht geändert werden.

`<check>false</check>`	Angabe zur Überprüfung der Verbindung zwischen dem Master-Admin-Server und dem Livelink-Server Mögliche Werte: `true` oder `false`

Angaben im Abschnitt <ldap>

Dieser Abschnitt enthält die Parameter für die Verbindung des Administrationsservers zum LDAP-Verzeichnisdienst.

Hinweise:

Beachten Sie auch die Informationen zu diesen Parametern in den Abschnitten “Parameter des LDAP-Verzeichnisdienstes einstellen” auf Seite 88 und “WCM-spezifische LDAP-Parameter angeben” auf Seite 90.

Das Mapping von WCM- auf LDAP-Attribute erfolgt ebenfalls über Einträge in der Datei **defaults.xml**, siehe Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45.

Tabelle 18 – Angaben im Abschnitt <ldap>

Eintrag in der XML-Datei	Erläuterung
<poolname>userpool</poolname>	Name des LDAP-Pools, der für die Verbindungen zum LDAP-Verzeichnisdienst angelegt wird
<provider>com.sun.jndi.ldap.LdapCtxFactory</provider>	Treiber für die Verbindung zum LDAP-Verzeichnisdienst Möglicher Wert: com.sun.jndi.ldap.LdapCtxFactory
<searchbase>ou=software solutions, o=company.example</searchbase>	Suchknoten. Mit diesem Parameter wird die Suche auf bestimmte Zweige des LDAP-Verzeichnisdienstes eingegrenzt.
<searchlimit>1000</searchlimit>	Maximale Anzahl an Ergebnissen, die Livelink WCM Server bei einer Suche im Verzeichnisdienst abholt

Eintrag in der XML-Datei	Erläuterung
`<authentication>simple</authentication>`	Verfahren für die Authentifizierung durch den LDAP-Verzeichnisdienst Möglicher Wert: `simple`
`<url>ldap://LDAPserver.company.example:389</url>`	Adresse für den Zugriff auf den LDAP-Server
`<user>cn=admin, o=company.example</user>`	Distinguished name des Benutzers für das LDAP-Bindeprofil, das vom WCM-System für die Anmeldung beim LDAP-Verzeichnisdienst verwendet wird
`<password>adminadmin</password>`	Passwort des LDAP-Bindeprofils
`<userclass>vipUser</userclass`	LDAP-Objektklasse zur Speicherung der Benutzer Standardwert: `vipUser`
`<groupclass>vipGroup</groupclass>`	LDAP-Objektklasse zur Speicherung der Gruppen Standardwert: `vipGroup`
`<roleclass>vipRole</roleclass>`	LDAP-Objektklasse zur Speicherung der Rollen Standardwert: `vipRole`

Eintrag in der XML-Datei	Erläuterung
`<nestedgroups>false</nestedgroups>`	Angabe, ob implizite Zuordnungen von Benutzern zu Gruppen und Rollen im WCM-System berücksichtigt werden sollen (siehe Abschnitt 3.1 “Konzept der Sammelgruppen und Sammelrollen” auf Seite 38) Mögliche Werte: `true` oder `false`
`<secure>false</secure>`	Angabe, ob die Kommunikation mit dem LDAP-Server über gesicherte Verbindungen (Secure Socket Layer) erfolgen soll Mögliche Werte: `true` oder `false`
`<servertype>other</servertype>`	Angabe, ob Microsoft Active Directory verwendet wird Mögliche Werte: `ads` oder `other`

`<userclass.viptype></userclass.viptype>`
`<groupclass.viptype></groupclass.viptype>`
`<roleclass.viptype></roleclass.viptype>`
	Wert des Attributs `vipType` für den jeweiligen Principal-Typ. Diese Angabe ist z.B. hilfreich, wenn Sie die Benutzerinformationen aus Ihrem LDAP-Verzeichnisdienst für mehrere installierte WCM-Systeme verwenden. Mithilfe dieses Attributs lässt sich der Zugriff auf die einzelnen WCM-Systeme separat steuern.

`<check>true</check>`	Angabe zur Überprüfung der Verbindung zwischen dem Master-Admin-Server und dem LDAP-Server Mögliche Werte: `true` oder `false`

Installation über die Konsole starten

Hinweis: Bitte beachten Sie auch die Informationen im Abschnitt “Hinweise zur Installation” auf Seite 72.

- **Windows:** Öffnen Sie die MS-DOS-Eingabeaufforderung, wechseln Sie auf das CD-ROM-Laufwerk bzw. das Verzeichnis mit den Installationsdateien. Rufen Sie das Skript mit dem Pfad auf Ihr Java 2 SDK-Verzeichnis und den Pfad auf die Datei **defaults.xml** (inklusive Dateiname) auf:

```
installConsole.bat {SDK-Installationsverzeichnis}\bin
   {Pfad zur Datei defaults.xml}
```

- **UNIX:** Im Wurzelverzeichnis der WCM-CD befindet sich ein JAR-Archiv, das Sie auf Ihren Server übertragen und in ein temporäres Verzeichnis entpacken müssen. Wechseln Sie in dieses Verzeichnis, und rufen Sie von dort aus das Installationsskript mit dem Pfad auf Ihr Java 2 SDK-Verzeichnis und dem Pfad zur Datei **defaults.xml** (inklusive Dateiname) als Parameter auf.

```
sh ./installConsole.sh [-jdk {SDK-Installationsverzeichnis}/bin]
   [-defaults {Pfad zur Datei defaults.xml}]
```

  Wenn Sie das Installationsskript ohne Parameter aufrufen, werden Sie anschließend aufgefordert, den Pfad auf Ihr Java 2 SDK-Verzeichnis (**{SDK-Installationsverzeichnis}/bin**/) und die Datei **defaults.xml** einzugeben.

Die Parameter für die Installation werden aus der Datei **defaults.xml** gelesen. Für alle Komponenten, die installiert werden sollen, muss im entsprechenden Absatz im Tag `<install_option>` der Wert `install` eingetragen werden. Für Komponenten, die weder installiert noch deinstalliert werden sollen, ist in diesem Tag `none` einzutragen (siehe Abschnitt “Parameter in der Datei `defaults.xml`” ab Seite 135.

Die Ergebnisse der Installation können Sie dem Installationsprotokoll entnehmen, siehe Abschnitt 4.10 “Protokoll- und Fehlerdateien” auf Seite 174.

Deinstallation über die Konsole starten

> **Hinweis:** Bitte beachten Sie auch die Informationen im Abschnitt “Hinweise zur Deinstallation” auf Seite 131.

- **Windows:** Öffnen Sie die MS-DOS-Eingabeaufforderung, wechseln Sie auf das CD-ROM-Laufwerk bzw. das Verzeichnis mit den Installationsdateien. Rufen Sie das Skript mit dem Pfad auf Ihr Java 2 SDK-Verzeichnis und den Pfad zur Datei **defaults.xml** (inklusive Dateiname) auf:

```
uninstallConsole.bat {SDK-Installationsverzeichnis}\bin
   {Pfad zur Datei defaults.xml}
```

- **UNIX:** Im Wurzelverzeichnis der WCM-CD befindet sich ein JAR-Archiv, das Sie auf Ihren Server übertragen und in ein temporäres Verzeichnis entpacken müssen. Wechseln Sie in dieses Verzeichnis, und rufen Sie von dort aus das Deinstallationsskript mit dem Pfad auf Ihr Java 2 SDK-Verzeichnis und dem Pfad zur Datei **defaults.xml** (inklusive Dateiname) als Parameter auf.

```
sh ./uninstallConsole.sh -[jdk {SDK-Installationsverzeichnis}/bin]
   [-defaults {Pfad zur Datei defaults.xml}]
```

Wenn Sie das Deinstallationsskript ohne Parameter aufrufen, werden Sie anschließend aufgefordert, den Pfad auf Ihr Java 2 SDK-Verzeichnis (**{SDK-Installationsverzeichnis}/bin**/) und die Datei **defaults.xml** einzugeben.

Die Parameter für die Deinstallation werden aus der Datei **defaults.xml** gelesen. Für alle Komponenten, die entfernt werden sollen, muss im entsprechenden Absatz im Tag `<install_option>` der Wert `uninstall` eingetragen werden. Für Komponenten, die weder installiert noch deinstalliert werden sollen, ist in diesem Tag `none` einzutragen (siehe Abschnitt “Parameter in der Datei `defaults.xml`” ab Seite 135.

Die Ergebnisse der Deinstallation können Sie dem Protokoll entnehmen, siehe Abschnitt 4.10 “Protokoll- und Fehlerdateien” auf Seite 174.

4.9 Server starten und stoppen

Die Server des WCM-Systems müssen nur einmal gestartet werden und sollten anschließend ständig in Betrieb sein. Es bietet sich an, diese als Hintergrundprozesse auszuführen. Wichtig ist dabei, dass der Benutzer, unter dessen Namen die Prozesse gestartet werden, über die erforderlichen Schreib- und Leseberechtigungen in den entsprechenden WCM-Verzeichnissen verfügt (siehe Abschnitt “Schreibrechte für die Verzeichnisse von Livelink WCM Server” auf Seite 126.

Bei der Installation des WCM-Systems und bei der nachträglichen Installation von Admin-Servern, Content-Servern und Suchservern werden Skripte zum Starten und Stoppen der Server eingerichtet. Das Vorgehen beim Starten bzw. Stoppen der verschiedenen Server unterscheidet sich:

- Admin- und Content-Server starten und stoppen (siehe Abschnitt “Server starten” auf Seite 163 und “Server stoppen” auf Seite 169)
- Content-Server starten, der im Kontext einer JSP-Engine bzw. als Webanwendung in einem Application-Server ausgeführt wird (siehe Abschnitt “Content-Server im Application-Server starten” auf Seite 170)
- Suchserver starten (siehe Abschnitt “Suchserver starten” auf Seite 172)

Achtung! Die mitgelieferten Start- und Stoppskripte für UNIX entsprechen dem Standard POSIX bzw. IEEE Std 1003.1-2001 (siehe http://www.opengroup.org/onlinepubs/007904975/toc.htm). Die Skripte müssen gegebenenfalls der verwendeten UNIX-Variante, der Version des Betriebssystems und der Shell angepasst werden.

Server starten

Achtung! Die Server dürfen nur unter dem Benutzernamen gestartet werden, unter dem sie installiert wurden. Sie sollten **nicht** unter der Benutzerkennung des Administrators gestartet werden. Unter UNIX sollten die Server grundsätzlich nicht mit der uid “0” bzw. “root” betrieben werden.

Fahren Sie zuerst den Admin-Server über **{Admin-Server-Name}.bat** bzw. **{Admin-Server-Name}.sh** hoch. Direkt nach der Installation läuft dieser bereits automatisch. Anschließend können die Server gesammelt über ein Startskript oder über separate Startskripte gestartet werden.

Die folgenden Hinweise gelten für Admin- und Content-Server. Gesonderte Hinweise zu Content-Servern, die im Kontext einer JSP-Engine bzw. als Webanwendung in einem Application-Server ausgeführt werden, und zu Suchservern erhalten Sie in den Abschnitten “Content-Server im Application-Server starten” auf Seite 170 und “Suchserver starten” auf Seite 172.

Server gesammelt starten

Zum Starten aller Server (außer dem Admin-Server, der bereits laufen muss), steht das Skript **startvip.bat** bzw. **startvip.sh** zur Verfügung.

- **Windows:** Öffnen Sie (z.B. im Windows Explorer) das WCM-Installationsverzeichnis, und führen Sie das Skript **startvip.bat** aus.
- **UNIX:** Wechseln Sie in das WCM-Installationsverzeichnis, und rufen Sie von dort das Skript auf:

```
sh ./startvip.sh
```

  Unter UNIX können Sie die Startdateien der Server auch als ausführbare Programme kennzeichnen. Zu diesem Zweck dient die Datei **set_executable.sh**, die sich im WCM-Installationsverzeichnis befindet. Führen Sie diese Datei vor dem Starten des HTTP-Servers, der JSP-Engine und des Admin-Servers aus.

  Der Aufruf des Startskripts lautet dann:

```
./startvip.sh
```

> **Hinweis:** Wenn Sie die Server unter UNIX betreiben, achten Sie darauf, dass die Anzahl der Datei-Deskriptoren, die dem Java-Prozess zur Verfügung stehen, mindestens 1024 betragen muss.

Server einzeln starten

Für das separate Starten einzelner Server gibt es folgende Möglichkeiten:

- Starten über das servereigene Startskript **{Servername}.bat** bzw. **{Servername}.sh**
- Starten über das Skript **startserver.bat** bzw. **startserver.sh**

Starten über servereigene Startskripte

Um einzelne Server zu starten, führen Sie das entsprechende Skript auf der Konsole aus. Das Skript ist nach dem Server benannt – heißt der Master-Content-Server z. B. “Master-Content”, hat das zugehörige Skript den Namen **Master-Content.bat** bzw. **Master-Content.sh**.

Beispiel – Startskript eines Master-Content-Servers (es werden die Standard-Ports des Admin-Servers verwendet):

```
d:
cd "d:\wcm"

call "d:\wcm\setClasspath.bat"

start "Master-Content" java -Xmx512m -Dvip.class.path=%VIPCLASSPATH%
  de.gauss.vip.contentmanager.server.ServerStarter
    -name Master-Content -admin {Admin-Host} -vipp 5002 -http 5003
      -language de_DE -secure false

exit
```

Die Startskripte werden bei der Installation der Server automatisch erstellt. Die folgende Tabelle gibt einen Überblick über die erforderlichen und möglichen Parameter in den Startskripten der Server.

Tabelle 19 – Parameter in den Startskripten der Server

Parameter	Erläuterung	Optional
`-Xmx512m`	Gibt die maximale Größe des Arbeitsspeichers in Megabyte an, die der Server beanspruchen darf **Hinweis:** Achten Sie bei der Installation mehrerer Server auf einem Rechner darauf, dass der Gesamtwert aller installierten Server nicht die Größe des virtuellen Speichers überschreitet.	
`-Dvip.vipsecure.debug=true`	Muss vor dem Klassennamen `de.gauss.vip.contentmanager.server.ServerStarter` in der Startdatei eingetragen werden Wenn dieser Parameter angegeben ist, werden die Anfragen und Antworten zwischen diesem Server und Secure Access in der Protokolldatei **{Servername}_out.log** protokolliert.	✓
`-name`	Name des Servers	
`-admin`	(nicht für Administrationsserver verfügbar) Name des Rechners, auf dem der zuständige Admin-Server installiert ist	
`-vipp`	(nicht für Administrationsserver verfügbar) VIPP-Port des Admin-Servers	
`-http`	(nicht für Administrationsserver verfügbar) HTTP-Port des Admin-Servers	

Parameter	Erläuterung	Optional
`-language`	Standardsprache des Servers Wert: `de_DE` oder `en_US`	
`-secure`	Verwendung von SSL `true` – SSL wird verwendet `false` – SSL wird nicht verwendet	
`-?` `-help`	Ausdruck der Aufrufparameter (Hilfetext) und Verlassen des Skripts	✓
`-console`	Ermöglicht die Eingabe von Befehlen über die Konsole (Debugging)	✓
`-installdir`	Installationsverzeichnis	
`-logsize`	Maximale Größe der Protokolldateien von Livelink WCM Server in KB Standard = 10240, Minimum = 5	✓
`-maxlogs`	Anzahl der Protokolldateien, die gespeichert bleiben sollen Standard = 3, Minimum = 0	✓
`-noredirect`	Meldungen werden nicht in den Protokolldateien protokolliert, sondern auf der Konsole ausgegeben.	✓

Starten über das Skript `startserver.bat` (bzw. `.sh`)

Alternativ können Sie einzelne Server auch über das Skript **`startserver.bat`** bzw. **`.sh`** starten.

Das Skript **startserver** (mit Standard-Ports des Admin-Servers):

```
d:
cd "d:\wcm"

call "d:\wcm\setClasspath.bat"

SET SERVERNAME=%1%

if "%SERVERNAME%" == "" goto ERROR

start "%SERVERNAME%" java -Xmx256m -Dvip.class.path=%VIPCLASSPATH%
    de.gauss.vip.contentmanager.server.ServerStarter -name %SERVERNAME%
      -admin {Admin-Host} -vipp 5002 -http 5003 -language de_DE
          -secure false

exit

:ERROR
echo improper call to this batch.
echo usage: "startserver <servername>"
```

Die einzelnen Parameter in dem Skript entsprechen den Angaben in den servereigenen Startskripten, siehe Tabelle 19 “Parameter in den Startskripten der Server” auf Seite 166.

So starten Sie einen Server mit diesem Skript:

1. Öffnen Sie die Konsole.
2. Wechseln Sie in das WCM-Installationsverzeichnis.
3. Geben Sie ein:

   ```
   startserver {Servername}
   ```

   also z.B.:

   ```
   startserver Admin
   ```

Server stoppen

Zum Herunterfahren der Server stehen die Skripte **shutdown_{Servername}.bat** bzw. **shutdown_{Servername}.sh** zur Verfügung. Alternativ dazu können Sie die Server auch über den Admin-Client beenden.

Tabelle 20 – Parameter in den Stoppskripten der Server

Parameter	Erläuterung	Optional
`-HOSTNAME`	Voll qualifizierter Hostname des Rechners, auf dem der Server installiert ist	
`-vipp`	VIPP-Port des Servers	
`-HTTP`	HTTP-Port des Servers	
`-SECURE`	Verwendung von SSL `true` – SSL wird verwendet `false` – SSL wird nicht verwendet	
`-DATA`	Vollständiger Pfad zu der Datei, die das verschlüsselte Einmalpasswort enthält	
`-runlevel`	Runlevel, auf den der Server gesetzt werden soll. Es ist auch möglich, den Server über diesen Parameter wieder hochzufahren. Der Standardwert ist 0 = “Server nicht erreichbar”.	✓
`-website`	Website, auf die sich der im Parameter `-runlevel` gesetzte Wert bezieht Der Standardwert ist “alle Websites”.	✓

Hinweise

- Die Stoppskripte sind mithilfe eines Einmalpassworts gegen Manipulationen gesichert.
- Wenn Sie einen Administrationsserver mithilfe des Skripts herunterfahren, laufen die anderen Server weiter. Es ist jedoch ohne einen laufenden Administrationsserver nicht möglich, sich am WCM-System anzumelden.
- WCM-Systeme, die von einem Proxy-Administrationsserver verwaltet werden, bleiben von Runlevel-Änderungen im Master-System unberührt.

Content-Server im Application-Server starten

Sowohl der Content-Client als auch der Content-Client (Classic) verwenden das Portal Manager API. Um dieses API – auch für selbsterstellte JSP-Seiten – zur Verfügung zu stellen, ist es erforderlich, einen Content-Server im Kontext des Application-Servers zu starten.

Content-Server als Webanwendung

Wenn für den Content-Server eine Webanwendung erzeugt wurde, läuft der Content-Server im Application-Server. Unterstützt der verwendete Application-Server den Servlet-Standard 2.3, wird der Content-Server automatisch zusammen mit der entsprechenden Webanwendung gestartet und gestoppt.

Unterstützt der Application-Server den Servlet-Standard 2.2, werden die Webanwendung und der Content-Server getrennt gestartet und gestoppt. Verwenden Sie in diesem Fall die entsprechenden Skripte für den Content-Server (siehe folgenden Abschnitt). Achten Sie darauf, dass die Webanwendung zuerst gestartet wird.

Content-Server in JSP-Engine starten

Wenn der Content-Server im Kontext einer JSP-Engine läuft, die keine Webanwendungen unterstützt, müssen zum Starten des Servers die im Verzeichnis **{WCM-Installationsverzeichnis}\tools** befindlichen Skripte verwendet werden.

Folgende Schritte sind dazu erforderlich:

1. Um den für den Content-Server benötigten Klassenpfad zu setzen, rufen Sie das Skript **setPomaClasspath.bat** bzw. **.sh** auf. Dieses Skript befindet sich im Verzeichnis **{WCM-Installationsverzeichnis}\tools**.
2. Fügen Sie den Klassenpfad, der durch das Aufrufen des Skipts erstellt wurde, dem Klassenpfad der JSP-Engine hinzu.
3. Kopieren Sie das mitgelieferte Skript **portalmanager.bat** bzw. **.sh** aus dem Verzeichnis **{WCM-Installationsverzeichnis}\tools** in das Wurzelverzeichnis der WCM-Installation; benennen Sie das Skript um in **{Name des Content-Servers}.bat** bzw **.sh**.
4. Ersetzen Sie im Skript **{Name des Content-Servers}.bat** bzw **.sh** alle Platzhalter `SERVERNAME` durch den Namen des Content-Servers.

Damit der Content-Server über das Skript gestartet werden kann, muss die JSP-Engine bereits laufen. In der Konfiguration der verwendeten JSP-Engine muss das Servlet-Mapping `'/servlet/*'` eingetragen sein (siehe auch die Beispielkonfiguration von Resin im Abschnitt “Datei resin.conf anpassen” auf Seite 188).

> **Hinweis:** Wenn Sie mehrere Content-Server auf demselben Rechner einrichten, müssen unterschiedliche JSP-Engines zum Ausführen der Server verwendet werden. Passen Sie in diesem Fall nach der Installation von Livelink WCM Server in den Skripten zum Starten der Content-Server die eingerichtete Standard-URL entsprechend der Konfiguration der verwendeten JSP-Engine an.

Zum Beenden des Content-Servers verwenden Sie das mitgelieferte Skript **shutdown_{Name des Content-Servers}.bat** bzw. **.sh**. Alternativ kann der Server auch über den Admin-Client heruntergefahren werden.

Suchserver starten

Content Miner-Suchserver

Wenn der Content Miner-Suchserver auf demselben Hostrechner wie der zugeordnete Content-Server installiert wurde, wird der Suchserver automatisch zusammen mit dem Server gestartet und gestoppt. In diesem Fall ist es außerdem möglich, den Suchserver über die Systemverwaltung des Admin-Client zu starten und zu stoppen. Damit der Suchserver gestartet werden kann, muss sich der zugeordnete Server mindestens im Runlevel 4 “Einzelnutzer-Betrieb” befinden. Weitere Informationen zur Vorgehensweise im Admin-Client finden Sie im Content Miner-Handbuch

Befinden sich Content Miner-Suchserver und zugeordneter Server auf unterschiedlichen Hostrechnern, können Sie den Suchserver über das mitgelieferte Startskript starten. Das Startskript **start_{Name des Suchservers}.bat** bzw. **.sh** befindet sich im Verzeichnis **{WCM-Installationsverzeichnis}\contentminer\{Name des Suchservers}\server**.

Hinweise

- Nach einer Neuinstallation kann der Startvorgang des Suchservers einige Zeit in Anspruch nehmen, da ein erstmaliges Initialisieren des Readware-Servers erforderlich ist.
- Beim Starten des Suchservers über das Startskript zeigt Ihnen folgende Meldung an, dass der Server hochgefahren ist: `Press “Ctrl C” to halt`.

- Wenn Sie den Suchserver unter Windows über das entsprechende Startskript starten, ist es nicht mehr möglich, diesen Suchserver mithilfe des Admin-Clients zu stoppen.
- Nach dem Zuordnen eines Suchservers zu einem Content-Server und nach dem Löschen aller Suchserver des WCM-Systems müssen der bzw. die entsprechenden Content-Server neu gestartet werden.

Unter UNIX haben Sie zusätzlich die Möglichkeit, das Index- und Query-System mithilfe von Skripten separat zu starten und auch zu stoppen. Zu diesem Zweck stehen Ihnen die folgenden Skripte zur Verfügung:

- Das Skript **start_{Name des Suchservers}_analyst.sh** startet nur das Index-System.
- Das Skript **start_{Name des Suchservers}_query.sh** startet nur das Query-System.
- Das Skript **stop_{Name des Suchservers}_analyst.sh** stoppt das Index-System.
- Das Skript **stop_{Name des Suchservers}_query.sh** stoppt das Query-System.

Lucene-Suchserver

Lucene-Suchserver können nur auf dem Hostrechner installiert werden, auf dem der zugeordnete Content-Server installiert ist. Sie werden immer automatisch zusammen mit dem Content-Server gestartet und gestoppt.

4.10 Protokoll- und Fehlerdateien

Bei allen Installations- und Deinstallationsvorgängen wird ein Protokoll in die Datei **{WCM-Installationsverzeichnis}\installation\ installation.log** geschrieben. Eventuell auftretende Fehler werden in die Datei **error.log** geschrieben, die sich in demselben Verzeichnis befindet.

Sämtliche Aktionen der Server werden in den Protokoll- und Fehlerdateien der entsprechenden Server gespeichert.

Wenn der Parameter `-noredirect` in den Startskripten der Server nicht gesetzt ist (siehe Tabelle 19 “Parameter in den Startskripten der Server” auf Seite 166), legt jeder Server in seinem **log**-Verzeichnis die Dateien **{Servername}_out.log** (für Standardmeldungen) und **{Servername}_err.log** (für Fehlermeldungen) an und schreibt die Protokolle in die Dateien.

Des Weiteren wird im **log**-Verzeichnis die Datei **{Servername}_com.log** angelegt, in die gegebenenfalls Kommunikationsfehler geschrieben werden.

> **Hinweis:** Die Protokolldateien der Server können auch über den Admin-Client eingesehen werden (siehe Livelink WCM Server-Administratorhandbuch).

Die Anzahl und Größe der Protokolldateien ist über die Parameter in den Startskripten der Server konfigurierbar (siehe Tabelle 19 “Parameter in den Startskripten der Server” auf Seite 166).

KAPITEL 5

Webserver einrichten

In Livelink WCM Server wird über eine URL auf die Objekte zugegriffen, um WCM-Objekte mit dem Content-Client zu bearbeiten und generierte Seiten über einen Browser anzuzeigen. Auf dem Rechner, auf dem sich der entsprechende WCM-Server befindet, muss dazu ein HTTP-Server installiert sein, der die Verzeichnisse der Deploymentsysteme auf die entsprechenden URLs umsetzt (mappt). Für den Betrieb verschiedener Komponenten des WCM-Systems (Content-Client und Content-Client (Classic), dynamisches Deployment und InSite Editing, WebDAV, Secure Access) ist außerdem eine JSP-Engine erforderlich. Die Konfigurationen von HTTP-Server und JSP-Engine müssen aufeinander abgestimmt sein.

> **Hinweis:** Der Prozess der JSP-Engine muss Schreibrechte für bestimmte Verzeichnisse haben. Beachten Sie dazu die Informationen im Abschnitt “Schreibrechte für die Verzeichnisse von Livelink WCM Server” auf Seite 126.

Zur Realisierung von HTTP-Diensten und Verarbeitung von JSP-Skripten können unterschiedliche Software-Produkte verwendet werden. Webserver vereinen die Funktionalitäten von HTTP-Servern und JSP-Engines. Sie können durch Application-Server oder eine Kombination aus HTTP-Server plus JSP-Engine realisiert werden.

In diesem Kapitel werden Hinweise zur Konfiguration von Webservern für die verschiedenen Komponenten von Livelink WCM Server anhand ausgewählter Beispiele gegeben. Hierzu werden die folgenden Beispielkonfigurationen beschrieben:

- Nutzung des HTTP-Servers Apache mit der JSP-Engine Tomcat (siehe folgenden Abschnitt)
- Nutzung des Application-Servers BEA WebLogic (siehe Abschnitt 5.2 “Szenario 2 – BEA WebLogic 8.1” auf Seite 183)
- Nutzung des HTTP-Servers Microsoft Internet Information Server mit der JSP-Engine Resin (siehe Abschnitt 5.3 “Szenario 3 – MS Internet Information Server mit Resin” auf Seite 185)

Um das Laden des Content-Clients zu beschleunigen, können Sie ein Precompile-Skript benutzen (siehe Abschnitt 5.4 “Das Precompile-Skript” auf Seite 202).

In einem separaten Abschnitt wird die Konfiguration für die Nutzung von Secure Access beschrieben (siehe Abschnitt 5.5 “Secure Access konfigurieren” auf Seite 203).

Hinweise

- In dieser Dokumentation kann nur die Konfiguration ausgewählter Webserver für bestimmte Anwendungsfälle beschrieben werden. Weitere Informationen und Konfigurationshinweise erhalten Sie in der Dokumentation des jeweiligen Produkts.
- Angaben zu den Versionsnummern der getesteten HTTP-Server und JSP-Engines, mit denen Livelink WCM Server zusammenarbeitet, sind in der Freigabemitteilung enthalten.
- Unterstützt der Web-Container des eingesetzten Application-Servers bzw. die JSP-Engine nur die Servlet-API 2.2, können in den Metadaten der WCM-Objekte keine Unicode-Zeichen verwendet werden. Aus diesem Grunde müssen Sie in diesem Fall Latin-1-Encoding für den Content-Client und die Website einstellen. Das Encoding für den Content-Client legen Sie bei der Installation des in der JSP-Engine laufenden Content-Servers fest, das Encoding für die Website beim Anlegen der Website.

- Bei der Installation des RDBMS Oracle unter Windows 2000 wird der HTTP-Server Apache automatisch mitinstalliert und als Dienst mit der Startart “Automatisch” eingetragen. Wenn Sie einen anderen HTTP- bzw. Webserver oder eine andere Apache-Konfiguration verwenden, deaktivieren Sie den eingerichteten Dienst oder deinstallieren Sie das Produkt.
- Zur Vermeidung von Problemen mit dem Content-Server, der im Kontext der JSP-Engine bzw. als Webanwendung in einem Application-Server läuft, sollte der Timeout-Wert der JSP-Engine auf denselben Wert gesetzt werden, den Livelink WCM Server zum automatischen Abmelden von Benutzern verwendet. Dieses *Ablaufintervall* wird in den Einstellungen des Administrationsservers auf dem Register *Administration* eingestellt.

  Wenn der Session-Timeout-Wert der JSP-Engine kleiner als das Ablaufintervall ist, werden möglicherweise mehr Lizenzen als erforderlich verwendet. Der Grund dafür ist, dass der Benutzer sich erneut beim Portal Manager API anmelden muss, wenn ein JSP-Session-Timeout eintritt, die Anmeldung bei Livelink WCM Server aber gültig bleibt. In diesem Fall werden zwei Lizenzen verwendet, bis die erste Anmeldung in Livelink WCM Server abläuft.

  Wenn der Wert des JSP-Session-Timeouts größer als der entsprechende Wert von Livelink WCM Server ist, wird eine `InvalidContextIdException` geworfen, falls ein Benutzer nicht aktiv war und in Livelink WCM Server ein Timeout eintritt, während die JSP-Session noch aktiv ist. Der JSP-Session-Timeout wird mithilfe des folgenden Parameters eingestellt:

```
<web-app app-dir='d:/wcm/website' id='/'>
   <session-config>
      <session-timeout>120</session-timeout>
   </session-config>
</web-app>
```

5.1 Szenario 1 – Apache 2 mit Tomcat

Voraussetzungen

- installierter HTTP-Server Apache 2 (hier: Version 2.0.55 für Windows)
- installierte JSP-Engine Tomcat (hier: Version 5.5.17)
- passendes JK-Plugin (jk-1.2.15, Datei **mod_jk-apache-2.0.55.so**)

  Das JK-Plugin ist für die Kommunikation zwischen Apache und Tomcat zuständig. Hierfür wird ein Tomcat-spezifisches Kommunikationsprotokoll verwendet.

  Das JK-Plugin steht als Download u.a. unter folgender URL zur Verfügung: http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/.

> **Hinweis:** Im hier beschriebenen Szenario wird davon ausgegangen, dass Apache 2 und Tomcat auf demselben Rechner installiert sind. Apache 2 benutzt den Port 80 für die HTTP-Verbindungen; dementsprechend darf dieser Port nicht von Tomcat verwendet werden.

Konfigurationsschritte

1. Stoppen Sie Apache und Tomcat.
2. Erzeugen Sie über den Admin-Client eine Webanwendung für die WCM-Server. (Detaillierte Informationen zum Vorgehen erhalten Sie im Abschnitt “Webanwendung erzeugen” auf Seite 101.)

   Geben Sie als Zielverzeichnis der erzeugten WAR-Datei das Verzeichnis **{Tomcat-Installationsverzeichnis}\webapps** an.

   Im Folgenden wird davon ausgegangen, dass der Name der Webanwendung “wcm” und der Name des Content-Clients “cmsclient” ist.

3. Installieren Sie das JK-Plugin. Benennen Sie dazu die Datei **mod_jk-apache-2.0.55.so** in **mod_jk.so** um und kopieren Sie sie in das Verzeichnis **{Apache 2-Installations-verzeichnis}\modules**.
4. Die Konfiguration von Apache 2 erfolgt in der Datei **httpd.conf** im Verzeichnis **{Apache 2-Installationsverzeichnis}\conf**. Fügen Sie der Datei im Abschnitt `LoadModule` die folgenden Zeilen hinzu:

```
LoadModule     jk_module  modules/mod_jk.so
JkWorkersFile  conf/workers.properties
JkLogFile      logs/mod_jk.log
JkLogLevel     info
JkLogStampFormat  "[%a %b %d %H:%M:%S %Y]"
JkOptions      +ForwardKeySize +ForwardURICompat -ForwardDirectories
JkRequestLogFormat "%w %V %T"
JkMount  /wcm/* worker1
```

5. Legen Sie im Verzeichnis **{Apache 2-Installationsverzeichnis}\conf** die Datei **workers.properties** mit folgendem Inhalt an:

```
worker.list=worker1
worker.worker1.type=ajp13
worker.worker1.host=localhost
worker.worker1.port=8009
worker.worker1.lbfactor=50
worker.worker1.cachesize=10
worker.worker1.cache_timeout=600
worker.worker1.socket_keepalive=1
worker.worker1.recycle_timeout=300
```

6. Starten Sie den Apache-Server und anschließend den Tomcat-Server.

   Beim Start wird automatisch die Webanwendung im Tomcat-Server installiert und gestartet.

HTTPS-Verbindung zum Content-Client verwenden

Sie können für die Verbindung zum Content-Client HTTPS nutzen. Da die Konfigurationsdateien des Content-Clients in dem Fall über einen HTTPS-Request geladen werden, ist es erforderlich, dem Truststore der JSP-Engine das Zertifikat des Webservers hinzuzufügen.

Hinweise zur Nutzung von Secure Access

- Allgemeine Informationen zu Secure Access erhalten Sie im Abschnitt 5.5 “Secure Access konfigurieren” auf Seite 203.
- Alle URLs, die dem in der Datei **httpd.conf** unter `JkMount` für das Tomcat-Plugin angegebenen Muster entsprechen (im Code-Beispiel alle mit dem Präfix “wcm/” beginnenden URLs), werden vom Apache 2-Server an den Tomcat-Server weitergeleitet. Die Funktionen der Zugriffssteuerungskomponente Secure Access werden vollständig im Tomcat-Server ausgeführt. Die Konfiguration von Secure Access erfolgt deshalb in der in Schritt 2 erzeugten Webanwendung (im Abschnitt `<filter>` der Datei **web.xml**).
- Um Secure Access nutzen zu können, setzen Sie in der Datei **web.xml** für den Secure Access-Filter den Parameter `pathto` auf den Wert `{Tomcat-Installationsverzeichnis}\webapps\`.

5.2 Szenario 2 – BEA WebLogic 8.1

Voraussetzung

Es werden sowohl der Webserver als auch die Servlet-Engine von BEA WebLogic 8.1 eingesetzt.

Konfigurationsschritte

1. Stoppen Sie WebLogic.
2. Erzeugen Sie über den Admin-Client eine Webanwendung für die WCM-Server. (Detaillierte Informationen zum Vorgehen erhalten Sie im Abschnitt “Webanwendung erzeugen” auf Seite 101.)

   Sofern Sie die Webanwendung nicht als Standardanwendung erzeugen, wird der Name der Webanwendung (z.B. wcm) Bestandteil der URL, mit der auf das WCM-System zugegriffen wird.

   Beispiel: http://wcmserver.company.example:7001/wcm
3. Legen Sie im Verzeichnis **{WebLogic-Installationsverzeichnis}\user_projects\mydomain\applications** ein Unterverzeichnis mit dem Namen der Webanwendung an.
4. Kopieren Sie die in Schritt 2 erzeugte WAR-Datei in das in Schritt 3 angelegte Verzeichnis, und entpacken Sie dort die WAR-Datei.

   Nach dem Entpacken befinden sich in diesem Verzeichnis die Unterverzeichnisse **\cmsclient**, **\htmlclient** und **\WEB-INF**.
5. Löschen Sie die WAR-Datei aus dem Verzeichnis.
6. Legen Sie über den Admin-Client Websites an. Berücksichtigen Sie dabei folgende Punkte:

- *Basis-URL:* Geben Sie zusätzlich zu der URL für das Deploymentsystem die Port-Nummer an, die der WebLogic-Server benutzt. Wenn Sie die Webanwendung nicht als Standardanwendung erzeugt haben, fügen Sie in die URL den Namen der Webanwendung ein.

  Beispiel: http://wcmserver.company.example:7001/wcm

- *Verzeichnis:* Geben Sie hier den Pfad auf das in Schritt 3 erzeugte Verzeichnis an.

Ausführliche Informationen zum Einrichten von Websites finden Sie im Livelink WCM Server-Administratorhandbuch.

7. Nur wenn die Webanwendung als Standardanwendung erzeugt wurde: Setzen Sie das URI-Präfix der Webanwendung auf "/". Legen Sie dazu im Verzeichnis **{WebLogic-Installationsverzeichnis}\user_projects\mydomain\applications\{Name der Webanwendung}\WEB-INF** die Datei **weblogic.xml** mit folgendem Inhalt an:

```
<weblogic-web-app>
   <context-root>/</context-root>
</weblogic-web-app>
```

HTTPS-Verbindung zum Content-Client verwenden

Sie können für die Verbindung zum Content-Client HTTPS nutzen. Da die Konfigurationsdateien des Content-Clients in dem Fall über einen HTTPS-Request geladen werden, ist es erforderlich, dem Truststore der JSP-Engine das Zertifikat des Webservers hinzuzufügen.

Hinweise zur Nutzung von Secure Access

- Allgemeine Informationen zu Secure Access erhalten Sie im Abschnitt 5.5 “Secure Access konfigurieren” auf Seite 203.
- Um Secure Access nutzen zu können, setzen Sie in der Datei **web.xml** für den Secure Access-Filter den Parameter `pathto` auf den Wert **{WebLogic-Installationsverzeichnis}\user_projects\mydomain\applications**.

5.3 Szenario 3 – MS Internet Information Server mit Resin

Die Konfiguration des Mappings von Verzeichnissen auf URLs für den HTTP-Server MS Internet Information Server (IIS) und die entsprechende Konfiguration für die JSP-Engine Resin wird für folgendes **Beispiel** beschrieben:

- Der Master-Content-Server ist auf dem Rechner mit dem Hostnamen “wcmserver.company.example” installiert.
- Die Website “InternetSite” wird angelegt.
- Auf dem Master-Content-Server befinden sich zwei Deploymentsysteme (Edit und QS) für diese Website.

  Die Daten der Deploymentsysteme werden im Verzeichnis **\website** unterhalb des WCM-Installationsverzeichnisses gespeichert. In diesem Verzeichnis werden zwei Unterverzeichnisse für die Deploymentsysteme Edit und QS angelegt:

  - Edit-Deploymentsystem: **d:\wcm\website\InternetSite_edit**
  - QS-Deploymentsystem: **d:\wcm\website\InternetSite_qs**

Ein Content-Server wird als Standardanwendung mit dem Namen “wcm” angelegt. Die Datei **wcm.war** wird in das Verzeichnis **d:\wcm\website** entpackt.

Folgende URLs werden im Admin-Client für den Zugriff auf die von den Deploymentsystemen erzeugten Seiten angegeben:

- Edit-Sicht: http://wcmserver.company.example/InternetSite_edit
- QS-Sicht: http://wcmserver.company.example/InternetSite_qs

MS Internet Information Server konfigurieren

So konfigurieren Sie das URL-Mapping in IIS:

1. Starten Sie den Internetdienste-Manager.
2. Markieren Sie links im Baum den Rechner, auf dem der WCM-Server installiert ist.
3. Markieren Sie im rechten Fensterbereich den Eintrag *Standardwebsite*, und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.
4. Geben Sie auf dem Register *Basisverzeichnis* im Feld *Lokaler Pfad* den lokalen Pfad für das URL-Mapping an.

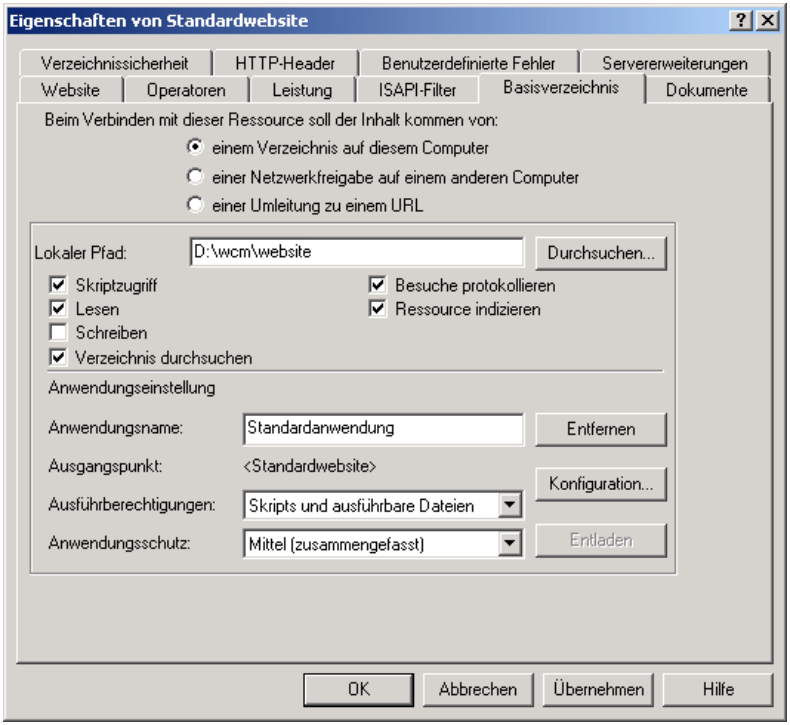


Abb. 20 – URL-Mapping in IIS

5. Bestätigen Sie die Einstellungen durch Klicken auf die Schaltfläche *OK*.

Resin konfigurieren

Im Folgenden werden die notwendigen Konfigurationsschritte für die JSP-Engine beschrieben, beginnend bei der Anmeldung der JSP-Engine am HTTP-Server. Die Beschreibung erfolgt am Beispiel der JSP-Engine Resin und des HTTP-Servers IIS (Version 5.0) unter Windows 2000.

Die Konfiguration von Resin beinhaltet folgende Schritte:

1. Datei **resin.conf** anpassen (siehe folgenden Abschnitt)
2. Resin in IIS einbinden (siehe Abschnitt “Resin in MS Internet Information Server einbinden” auf Seite 191)
3. Resin starten (siehe Abschnitt “Resin starten” auf Seite 191)

Datei resin.conf anpassen

Die grundsätzliche Konfiguration von Resin erfolgt über die Datei **resin.conf** im Verzeichnis **{Resin-Installationsverzeichnis}\conf**.

Der für Resin relevante WCM-Server ist eine Webanwendung, die über die Datei **web.xml** konfiguriert wird. Diese Datei wird beim Einrichten der Webanwendung automatisch erstellt und befindet sich im Verzeichnis **\WEB-INF** der Webanwendung (siehe Abschnitt “Webanwendung erzeugen” auf Seite 101).

Resin wird über ein Plugin (Datei **isapi_srun.dll**) in IIS eingebunden. Das Plugin entscheidet, welche Anfragen (URL-Requests) an Resin weitergeleitet werden und welche IIS auf andere Weise bedient. In der Datei **resin.conf** muss eine entsprechende Information hierzu hinterlegt sein.

Außerdem muss in der Datei **resin.conf** das Basis-Verzeichnis der Webanwendung angegeben sein. Das Basis-Verzeichnis können Sie entweder über das Tag `<war-dir>` oder das Tag `<app-dir>` festlegen.

- `<war-dir>`: Hier geben Sie das Verzeichnis an, in dem WAR-Dateien liegen, die Resin entpacken und als Webanwendung behandeln soll. Dieses Verzeichnis muss das Basis-Verzeichnis des HTTP-Servers sein.

Bei dieser Konfiguration ist es nicht möglich, das Website-Verzeichnis selbst als Verzeichnis für die sogenannte Standardanwendung zu nutzen. (Resin erwartet, dass die WAR-Datei einer Standardanwendung **root.war** heißt und entpackt die Webanwendung in ein Verzeichnis **root**.)

- `<app-dir>`: Hier geben Sie direkt ein Verzeichnis der Webanwendung an.

  Bei dieser Konfiguration ist es möglich, das Website-Verzeichnis selbst als Basis-Verzeichnis für die Webanwendung zu nutzen. Dafür muss die Datei **wcm.war** ohne Resin entpackt werden (z.B. durch Aufrufen des Befehls `jar –xf wcm.war` im Website-Verzeichnis). Die folgende Beispielkonfiguration verwendet diesen Ansatz.

Beispielkonfiguration

> **Hinweis:** Die folgende Beispielkonfiguration stellt nur die Informationen dar, die für die Integration von Resin mit IIS erforderlich sind.

Fügen Sie einen neuen `<web-app>`-Abschnitt in die Datei **resin.conf** ein. Tragen Sie in einem Abschnitt das Basis-Verzeichnis des HTTP-Servers als Applikationsverzeichnis ein, z.B. `<web-app app-dir= 'd:/wcm/website' id='/'>`.

In diesem Abschnitt erfolgt dann das Mapping für das Plugin. Sie können hier außerdem die Priorität des Plugins für IIS festlegen.

- Resin ohne Secure Access

```
<caucho.com>
<java compiler="internal" compiler-args=""/>
<!-- <iis priority='high'/> -->
<http-server class-update-interval='15'>
<srun port='6802'/>
<!-- VIP default -->
<web-app app-dir='d:/wcm/website' id='/'>
<!-- send to resin -->
<servlet-mapping url-pattern='*.jsp' servlet-name='plugin_match'/>
```

```
</web-app>
</http-server>
</caucho.com>
```

- Resin mit Secure Access

```
<caucho.com>
<java compiler="internal" compiler-args=""/>
<!-- <iis priority='high'/> -->
<http-server class-update-interval='15'>
<srun port='6802'/>
<!-- VIP default -->
<web-app app-dir='d:/wcm/website' id='/'>
<!-- send to resin -->
<servlet-mapping url-pattern='/*' servlet-name='plugin_match'/>
<!-- don't send to resin -->
<servlet-mapping url-pattern='/secret/*' servlet-
name='plugin_ignore'/>
<!-- if asp pages shall not be checked by Secure Access, hide them
from resin! -->
<!-- <servlet-mapping url-pattern='*.asp' servlet-
name='plugin_ignore'/> -->
</web-app>
</http-server>
</caucho.com>
```

Alias für Content-Client

Wenn Sie für den Content-Client einen Alias im HTTP-Server eingerichtet haben, muss dies auch in der Konfiguration der JSP-Engine eingetragen werden. Für Resin tragen Sie in diesem Fall folgende Zeilen in der Datei **resin.conf** ein:

```
<path-mapping url-pattern="/cmsclient/*"
real-path="{WCM-Installationsverzeichnis}/website/cmsclient" />
```

Resin in MS Internet Information Server einbinden

So binden Sie Resin in IIS ein:

1. Führen Sie die Datei **{Resin-Installationsverzeichnis}\bin\setup.exe** aus.
2. Stellen Sie sicher, dass IIS das Ausführen der Datei **isapi_srun.dll** im Skript-Verzeichnis erlaubt.

   Wählen Sie dazu im Dialog *Eigenschaften von Standardwebsite* auf dem Register *Basisverzeichnis* in der Auswahlliste *Ausführberechtigungen* den Eintrag *Skripts und ausführbare Dateien* (siehe Abbildung 20 “URL-Mapping in IIS” auf Seite 187).
3. Starten Sie IIS neu.

Resin starten

Als letzten Schritt der Resin-Konfiguration starten Sie Resin neu.

WCM-Server als Windows-Dienste installiert

Wenn die WCM-Server als Dienste installiert sind, empfiehlt es sich, für die JSP-Engine ebenfalls einen Dienst einzurichten. Führen Sie dazu folgenden Befehl aus:

```
{Resin-Installationsverzeichnis}\bin\httpd.exe –install-as resin
```

Konfigurieren Sie den Dienst anschließend so, dass zuerst der Administrationsserver gestartet wird und anschließend Resin. Implizit wird aufgrund der Angaben in der Datei **web.xml** mit Resin auch der Content-Server, der im Kontext der JSP-Engine bzw. als Webanwendung in einem Application-Server läuft, gestartet.

WCM-Server nicht als Windows-Dienste installiert

Wenn die WCM-Server nicht als Dienste installiert sind, muss die JSP-Engine (und damit auch der Content-Server, der im Kontext der JSP-Engine bzw. als Webanwendung in einem Application-Server läuft) nach dem Start des Administrationsservers durch folgenden Aufruf gestartet werden:

```
start "resin" {Resin-Installationsverzeichnis}\bin\httpd.exe
```

HTTPS-Verbindung zum Content-Client verwenden

Sie können für die Verbindung zum Content-Client HTTPS nutzen. Da die Konfigurationsdateien des Content-Clients in dem Fall über einen HTTPS-Request geladen werden, ist es erforderlich, dem Truststore der JSP-Engine das Zertifikat des Webservers hinzuzufügen.

Hinweise zur Nutzung von Secure Access

> **Hinweis:** Allgemeine Informationen zu Secure Access erhalten Sie im Abschnitt 5.5 “Secure Access konfigurieren” auf Seite 203.

Bei der Verwendung von IIS als HTTP-Server können verschiedene Authentifizierungsmethoden verwendet werden, wenn ein Benutzer auf ein Verzeichnis zugreift, das durch Secure Access geschützt ist:

- Base-Authentifizierung: Standard-Authentifizierung über den Anmeldedialog des Browsers (siehe Abschnitt “Base-Authentifizierung konfigurieren” auf Seite 193)

- NTLM-Authentifizierung (nur in Windows-Umgebungen bei Verwendung von IIS zusammen mit Internet Explorer): Zur Anmeldung am WCM-System werden die Benutzerdaten verwendet, mit denen sich der Benutzer am Windows-Betriebssystem angemeldet hat. Die Anmeldung am WCM-System erfolgt ohne Benutzereingaben im Hintergrund (siehe Abschnitt “NTLM-Authentifizierung konfigurieren” auf Seite 199).

Base-Authentifizierung konfigurieren

Bei einer Base-Authentifizierung erfolgt die Anmeldung am WCM-System über einen Anmeldedialog im Browser. Voraussetzung hierfür ist, dass in den Einstellungen der entsprechenden Pfade für Secure Access im Admin-Client unter *Anmeldemethode* die Option *base* ausgewählt ist (siehe Livelink WCM Server-Administratorhandbuch).

Die Base-Authentifizierung kann in IIS als anonymer Zugang oder Zugang über Benutzername und Passwort konfiguriert werden. In beiden Fällen ändert sich für den Benutzer beim Zugriff auf das WCM-System nichts – er muss in jedem Fall seine Benutzerdaten für das WCM-System im Anmeldedialog des Browsers eintragen.

Anonymer Zugang

So konfigurieren Sie den anonymen Zugang für die Base-Authentifizierung:

1. Starten Sie den Internetdienste-Manager.
2. Markieren Sie links im Baum den Rechner, auf dem der WCM-Server installiert ist.
3. Markieren Sie im rechten Fensterbereich den Eintrag *Standardwebsite*, und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.

4. Klicken Sie auf dem Register *Verzeichnissicherheit* im Bereich *Steuerung des anonymen Zugriffs und der Authentifizierung* auf die Schaltfläche *Bearbeiten*.

5. Aktivieren Sie im Dialog *Authentifizierungsmethoden* das Kontrollkästchen *Anonyme Anmeldung*.

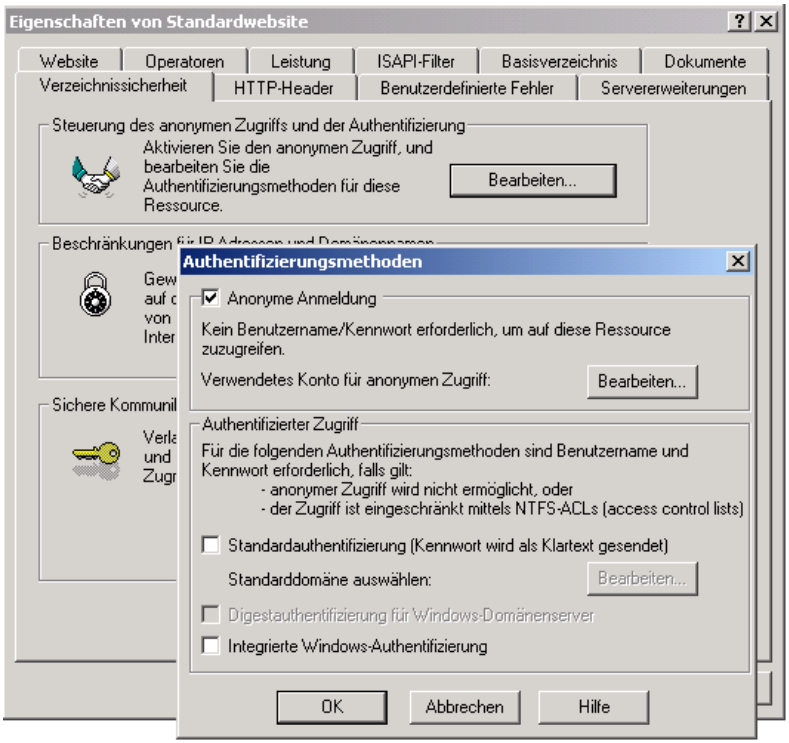


Abb. 21 – IIS-Konfiguration für Base-Authentifizierung mit anonymem Zugang

Zugang über Benutzername und Passwort

Voraussetzung für diese Konfiguration der Base-Authentifizierung ist, dass die Datei **VIPSecure.dll** als ISAPI-Filter für die geschützten Verzeichnisse konfiguriert ist. Diese Datei befindet sich auf der WCM-CD im Verzeichnis **\VipSecure\Binaries**.

Konfigurieren Sie die Datei **VIPSecure.dll** als ISAPI-Filter für die geschützten Verzeichnisse. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie den Internetdienste-Manager.
2. Markieren Sie links im Baum den Rechner, auf dem der WCM-Server installiert ist, und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.
3. Klicken Sie im Dialog *Eigenschaften* auf dem Register *Internet-Informationsdienste* im Bereich *Haupteigenschaften* auf die Schaltfläche *Bearbeiten*.
4. Klicken Sie im Dialog *Haupteigenschaften des WWW-Dienstes* auf dem Register *ISAPI-Filter* auf die Schaltfläche *Hinzufügen*.
5. Geben Sie im Dialog *Filtereigenschaften* den Namen des Filters und den Pfad zur Datei **VIPSecure.dll** an.

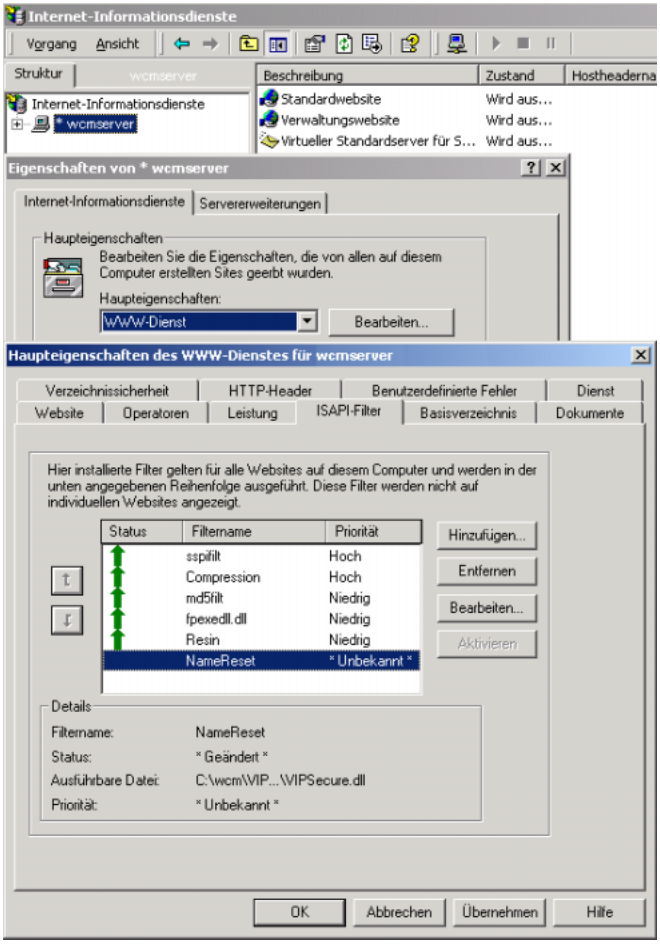


Abb. 22 – VIPSecure.dll als ISAPI-Filter konfigurieren (IIS)

Die DLL setzt den Namen und das Passwort, das der Benutzer im Browser für den Zugriff auf geschützte Dateien angibt, auf die Anmeldeinformationen eines Windows-Benutzers um. Diese Anmeldeinformationen werden in der Datei **vipsecure.ini** eingetragen.

1. Legen Sie die Datei **vipsecure.ini** an.
2. Tragen Sie folgenden Text in die Datei ein:

```
[ntlm]
user=
pwd=
```

3. Kopieren Sie die Datei in ein Windows-Verzeichnis, z. B. **C:\WINNT**. Dieses Verzeichnis muss über die Windows-System-umgebungsvariable PATH erreichbar sein.

So konfigurieren Sie den Zugang über Benutzername und Passwort für die Base-Authentifizierung:

1. Starten Sie den Internetdienste-Manager.
2. Markieren Sie links im Baum den Rechner, auf dem der WCM-Server installiert ist.
3. Markieren Sie im rechten Fensterbereich den Eintrag *Standardwebsite*, und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.
4. Klicken Sie auf dem Register *Verzeichnissicherheit* im Bereich *Steuerung des anonymen Zugriffs und der Authentifizierung* auf die Schaltfläche *Bearbeiten*.
5. Aktivieren Sie nur das Kontrollkästchen *Standardauthentifizierung (Kennwort wird als Klartext gesendet)*.

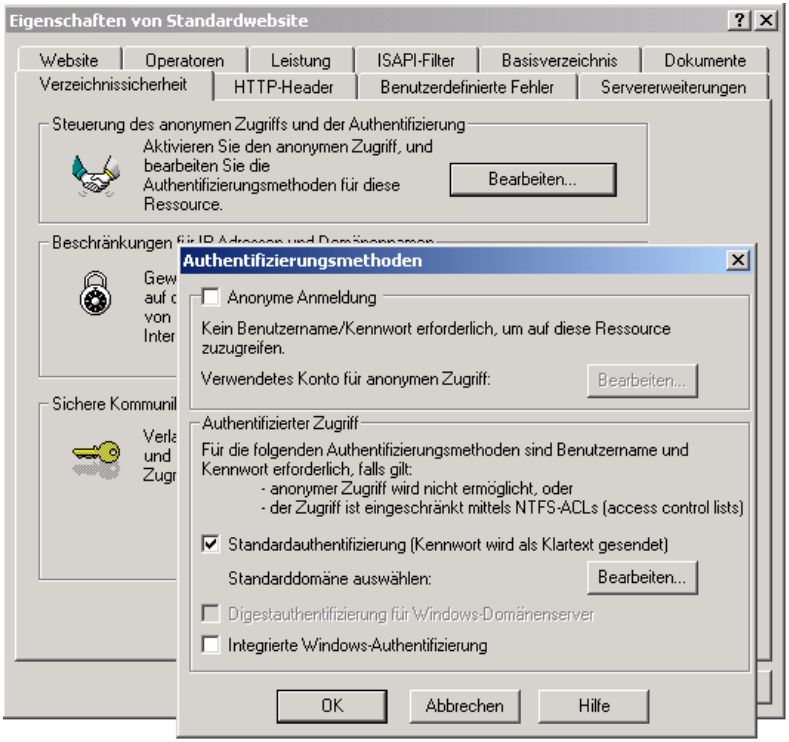


Abb. 23 – IIS-Konfiguration für Base-Authentifizierung mit Name und Passwort

6. Tragen Sie in der Datei **vipsecure.ini** die Anmeldedaten eines Benutzers ein, der auf diesem Rechner registriert ist und über entsprechende Zugriffsrechte im Dateisystem verfügt.

   Die Anmeldedaten, die der Benutzer beim Zugriff auf eine Secure Access-geschützte Datei eingibt, werden von der Datei **VipSecure.dll** auf diese Anmeldedaten umgesetzt.

NTLM-Authentifizierung konfigurieren

Alternativ zur Base-Authentifizierung kann das Verfahren NTLM genutzt werden. Wenn ein Benutzer eine geschützte Seite anfordert, werden seine Anmeldeinformationen vom Betriebssystem gelesen und die Anmeldung am WCM-System erfolgt im Hintergrund.

Voraussetzungen

- In den Einstellungen der entsprechenden Pfade für Secure Access im Admin-Client muss dazu unter *Anmeldemethode* die Option *ntlm* ausgewählt sein (siehe Livelink WCM Server-Administratorhandbuch).
- Verwenden Sie ein RDBMS zur Speicherung der Benutzerdaten, dann müssen die im Admin-Client konfigurierten Benutzerkennungen für das WCM-System als Windows-Benutzernamen existieren und den Namen der Windows-Domäne enthalten, z.B. “COMPANYDOMAIN\jstein”. Bei Verwendung eines LDAP-Verzeichnisdienstes kann die Domäne in den Einstellungen des Benutzers in einem separaten Feld eingetragen werden.
- In den Einstellungen der WCM-Benutzer im Admin-Client muss das Kontrollkästchen *Vertraute Anmeldung* aktiviert sein.
- Die **VipSecure.dll** darf **nicht** verwendet werden.

IIS und Internet Explorer konfigurieren

So konfigurieren Sie NTLM:

1. Starten Sie den Internetdienste-Manager.
2. Markieren Sie links im Baum den Rechner, auf dem der WCM-Server installiert ist.
3. Markieren Sie im rechten Fensterbereich den Eintrag *Standardwebsite*, und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.

4. Klicken Sie auf dem Register *Verzeichnissicherheit* im Bereich *Steuerung des anonymen Zugriffs und der Authentifizierung* auf die Schaltfläche *Bearbeiten*.
5. Aktivieren Sie die Kontrollkästchen *Anonyme Anmeldung* und *Integrierte Windows-Authentifizierung*.

> **Hinweis:** Wenn Sie nur das Kontrollkästchen *Integrierte Windows-Authentifizierung* aktivieren, schlagen interne URL-Verbindungen von Livelink WCM Server und Secure Access fehl. Dies führt dazu, dass das Ausleihen und Zurückgeben von WCM-Objekten mithilfe des Download-Applets, die Statifizierung und die Redirect- und Welcome-Page-Verarbeitung von Secure Access nicht funktionieren.

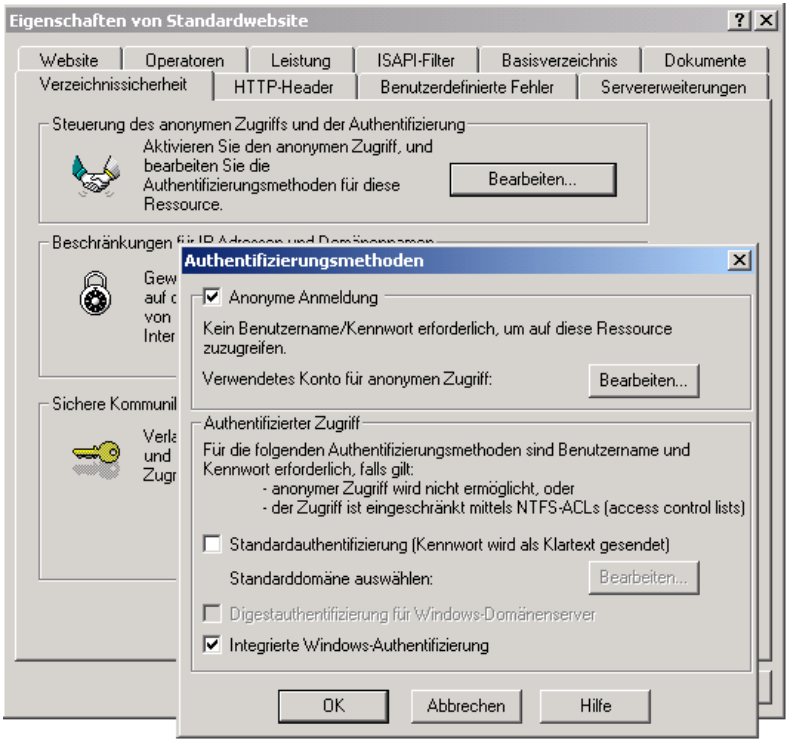


Abb. 24 – Konfiguration von IIS für NTLM-Authentifizierung

In den Einstellungen des Browsers, den die Benutzer verwenden, muss die automatische Anmeldung aktiviert werden. Dies erfolgt im Internet Explorer über *Extras* → *Internetoptionen* → Register *Sicherheit* → Schaltfläche *Stufe anpassen* → *Benutzerauthentifizierung* → Aktivieren des Optionsfelds *Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort*.

5.4 Das Precompile-Skript

Nach der Installation befindet sich im Verzeichnis **{WCM-Installationsverzeichnis}\tools** das Skript **precompile.bat** bzw. **precompile.sh**, das das Vorkompilieren des Content-Clients ermöglicht. Auf diese Weise wird der erste Zugriff auf den Content-Client beschleunigt.

Um das Skript ausführen zu können, müssen der Admin-Server, der Master-Content-Server, die JSP-Engine und der Content-Server, der im Kontext der JSP-Engine bzw. als Webanwendung in einem Application-Server läuft, gestartet sein.

Der Aufruf des Skripts erfolgt folgendermaßen:

```
precompile {Applikationsverzeichnis der JSP-Engine} {JSP-Basis-URL}
```

Die einzelnen Komponenten setzen sich wie folgt zusammen:

- `{Applikationsverzeichnis der JSP-Engine}`: Tragen Sie hier das Applikationsverzeichnis ein, das Sie in der Konfiguration der JSP-Engine für den Content-Client definiert haben.

  Beispiel: `d:/wcm/website/cmsclient`

- `{JSP-Basis-URL}`: URL, über die das angegebene Applikationsverzeichnis erreichbar ist. Das Mapping von Verzeichnis auf URL erfolgt in der Konfiguration des HTTP-Servers.

  Beispiel: `http://wcmserver.company.example/cmsclient`

Das Skript sollte nach *jedem* Neustart der JSP-Engine ausgeführt werden, bevor die Benutzer beginnen, mit dem Content-Client zu arbeiten.

5.5 Secure Access konfigurieren

Die an einen Content-Server gebundenen Deploymentsysteme erzeugen in den konfigurierten Verzeichnissen die HTML-Dateien, JSP-Seiten etc. Auf diese Verzeichnisse kann über einen HTTP-Server und einen Webbrowser zugegriffen werden.

Um die generierten Dateien vor unberechtigten Zugriffen, z.B. über das Internet, zu schützen, können Sie Teile oder alle Verzeichnisse eines Deploymentsystems mithilfe von Secure Access überwachen lassen. Dies bietet die Möglichkeit, die Zugriffssteuerung, die für die Arbeit an einem WCM-Objekt im Content-Client gilt, auf den Webserver bzw. die JSP-Engine zu übertragen. Damit ist im Produktionsbetrieb (also auch im Internet) eine objektspezifische Zugriffssteuerung auf alle Objekte einer Website möglich.

Dynamische Deploymentsysteme müssen nicht durch Secure Access geschützt werden. Den Zugriffsschutz übernehmen die für das dynamische Deployment eingesetzten Servlets.

Funktionsweise

Secure Access ist als Servlet bzw. Filter implementiert und läuft in der JSP-Engine. Wird über einen Browser vom HTTP-Server eine Seite angefordert und reicht der HTTP-Server die Anfrage an die JSP-Engine weiter, fängt Secure Access diese Anfrage ab und überprüft, ob die Anfrage einem der konfigurierten geschützten Verzeichnisse gilt. Ist dies der Fall, erhält der Benutzer einen Anmeldedialog im Browser, in den er seine Benutzerkennung und das Passwort für den Zugriff auf das WCM-System eintragen muss.

Alternativ zur Anmeldung im Browser können für die Authentifizierung des Benutzers auch die Anmeldeinformationen des Windows-Betriebssystems verwendet werden. Dies ist möglich, wenn Sie das WCM-System in einer Windows-Domäne betreiben, den MS Internet Information Server als Webserver und den MS Internet Explorer als Browser einsetzen. In den Einstellungen der Pfade für Secure Access können Sie für diesen Fall die Anmeldemethode *ntlm* auswählen. Zur Konfiguration von NTLM siehe Abschnitt “NTLM-Authentifizierung konfigurieren” auf Seite 199.

Die Anmeldedaten werden vom Admin-Server des WCM-Systems überprüft. War die Anmeldung des Benutzers erfolgreich, wird die Anzeige der Seiten über den HTTP-Server erlaubt und der Benutzer kann das Objekt im Browser betrachten.

Notwendige Konfiguration

Um Secure Access nutzen zu können, sind folgende Arbeiten notwendig:

- Aktivieren von Secure Access und Hinzufügen der Pfade für Secure Access im Admin-Client (siehe folgenden Abschnitt)
- Anmelden der JSP-Engine am HTTP-Server (siehe Abschnitt 5.1 “Szenario 1 – Apache 2 mit Tomcat” auf Seite 180 und Abschnitt 5.3 “Szenario 3 – MS Internet Information Server mit Resin” auf Seite 185)
- Konfigurieren der Secure Access-Parameter (siehe Abschnitt “Gemeinsame Parameter für das Secure Access-Servlet und den Secure Access-Filter” ab Seite 211) und Einkommentieren der Einträge in der Datei **web.xml**

Sie haben außerdem die Möglichkeit, die HTTP-Requests für geschützte Seiten mithilfe einer Java-Klasse nachzubearbeiten. Auf diese Weise können Sie z. B. eine automatische Anmeldung von Benutzern auf Grundlage ihrer IP-Adresse ermöglichen. Siehe dazu Abschnitt “HTTP-Requests für geschützte Seiten nachbearbeiten” auf Seite 224.

Einstellungen im Admin-Client

Die Zugriffsschutzkomponente Secure Access muss für den Server aktiviert werden, über dessen Deploymentsysteme die zu schützenden Dateien publiziert werden. Das setzt voraus, dass diese Deploymentsysteme bereits angelegt sind. Um Secure Access für einen Server zu aktivieren, sind folgende Einstellungen im Admin-Client notwendig:

Secure Access in den Server-Einstellungen aktivieren

So aktivieren Sie Secure Access in den Server-Einstellungen:

1. Öffnen Sie die Einstellungen des Servers über *Konfiguration* → *Server* → *{Servername}*.
2. Aktivieren Sie auf dem Register *Secure Access* das Kontrollkästchen *Secure Access aktiv*.
3. Tragen Sie auf Register *Secure Access* im Feld *Webserver* den Name des verwendeten HTTP-Servers ein. Dieser Name muss mit dem Namen übereinstimmen, den Sie bei der Konfiguration der JSP-Engine im Parameter `profile` eintragen (siehe Abschnitt “Gemeinsame Parameter für das Secure Access-Servlet und den Secure Access-Filter” auf Seite 211).

Pfade für Secure Access hinzufügen

Um die Dateien in einem Deploymentsystemverzeichnis schützen zu lassen, muss der Pfad zu diesem Verzeichnis registriert werden.

So fügen Sie Pfade für Secure Access hinzu:

1. Öffnen Sie *Konfiguration* → *Server* → *{Servername}* → *Pfade für Secure Access*.
2. Tragen Sie ein, welche Verzeichnisse durch Secure Access geschützt werden sollen.

Hinweise:

Ausführliche Informationen zur Konfiguration von Secure Access über den Admin-Client enthält das Livelink WCM Server-Administratorhandbuch (Kapitel “Server verwalten”).

Nach dem Hinzufügen von Pfaden für Secure Access über den Admin-Client muss die JSP-Engine neu gestartet werden, damit diese die neue Konfiguration lesen kann.

HTTP-Server für Secure Access konfigurieren

Der HTTP-Server muss so konfiguriert werden, dass alle eingehenden Anfragen an die JSP-Engine weitergeleitet werden.

Szenario 1 – Apache mit Tomcat

Alle URLs, die dem in der Datei **httpd.conf** unter `JkMount` für das Tomcat-Plugin angegebenen Muster entsprechen, werden vom Apache-Server an den Tomcat-Server weitergeleitet. Die Funktionen der Zugriffssteuerungskomponente Secure Access werden vollständig im Tomcat-Server ausgeführt.

Szenario 2 – BEA WebLogic 8.1

Sie können Secure Access für BEA WebLogic 8.1 nutzen, ohne spezielle Konfigurationseinstellungen vornehmen zu müssen.

Szenario 3 – MS Internet Information Server mit Resin

Informationen zum Anmelden von Resin an IIS erhalten Sie im Abschnitt “Resin in MS Internet Information Server einbinden” auf Seite 191. Mit dem dort beschriebenen Vorgehen wird die JSP-Engine allgemein in den HTTP-Server eingebunden, sodass dies keine Secure Access-spezifische Konfiguration ist.

Hinweis: Informationen zur Konfiguration der verschiedenen Anmeldemethoden (“base” und “ntlm”) für IIS erhalten Sie im Abschnitt “Hinweise zur Nutzung von Secure Access” ab Seite 192.

JSP-Engine für Secure Access konfigurieren

Die Parameter für das Secure Access-Servlet bzw. den Secure Access-Filter werden in den Einstellungen der verwendeten JSP-Engine konfiguriert.

Hinweis: Das Secure Access-Servlet und der Secure Access-Filter bieten denselben Funktionsumfang. Um den Filter nutzen zu können, dessen Konfiguration einfacher ist, muss die JSP-Engine jedoch die JSP-Spezifikation 2.3 unterstützen. Für das Servlet ist 2.2 ausreichend.

Die Konfiguration für Secure Access wird beim Einrichten des Content-Servers als Webanwendung in der Datei **web.xml** automatisch vorgenommen. Im Allgemeinen ist es erforderlich, den Parameter `pathto` anzupassen. Der Wert dieses Parameters muss das Basisverzeichnis des HTTP-Servers sein.

Für das Secure Access-Servlet werden in der Datei **web.xml** folgende Einträge generiert. (Bitte beachten Sie, dass die Parameter wie z.B. Servername, Verzeichnisse und Port-Nummern von den Angaben beim Erzeugen der Webanwendung abhängen.)

```
<!--
<servlet>
      <servlet-name>AccessServlet</servlet-name>
      <servlet-class>de.gauss.vip.vipsecure.AccessServlet
         </servlet-class>
      <init-param>
         <param-name>character-encoding</param-name>
         <param-value>UTF-8</param-value>
      </init-param>
      <init-param>
         <param-name>pathfrom</param-name>
         <param-value></param-value>
      </init-param>
      <init-param>
         <param-name>pathto</param-name>
         <param-value>d:/wcm/website</param-value>
      </init-param>
      <init-param>
         <param-name>usepath</param-name>
         <param-value>false</param-value>
      </init-param>
      <init-param>
         <param-name>viphost</param-name>
         <param-value>wcmserver.company.example</param-value>
      </init-param>
      <init-param>
         <param-name>vippport</param-name>
         <param-value>5008</param-value>
      </init-param>
      <init-param>
         <param-name>httpport</param-name>
         <param-value>5009</param-value>
      </init-param>
      <init-param>
         <param-name>secure</param-name>
         <param-value>false</param-value>
      </init-param>
      <init-param>
         <param-name>profile</param-name>
         <param-value>wcm</param-value>
      </init-param>
      <init-param>
         <param-name>loglevel</param-name>
         <param-value>0</param-value> <!-- 191 -->
      </init-param>
      <init-param>
         <param-name>realm</param-name>
```

```
         <param-value>WCM</param-value>
      </init-param>
      <init-param>
         <param-name>logdir</param-name>
         <param-value>d:/wcm/log</param-value>
      </init-param>
      <init-param>
         <param-name>logname</param-name>
         <param-value>servlet_1</param-value>
      </init-param>
</servlet>
-->

<!--
<servlet-mapping>
      <servlet-name>AccessServlet</servlet-name>
      <url-pattern>/*</url-pattern>
</servlet-mapping>
-->
```

Für den Secure Access-Filter werden in der Datei **web.xml** z.B. für die JSP-Engine Resin folgende Einträge generiert:

```
<!--
<filter>
      <filter-name>AccessFilter</filter-name>
      <filter-class>de.gauss.vip.vipsecure.AccessFilter</filter-class>
         <init-param>
            <param-name>character-encoding</param-name>
            <param-value>UTF-8</param-value>
         </init-param>
         <init-param>
            <param-name>pathfrom</param-name>
            <param-value></param-value>
         </init-param>
         <init-param>
            <param-name>pathto</param-name>
            <param-value>d:/wcm/website</param-value>
         </init-param>
         <init-param>
            <param-name>usepath</param-name>
            <param-value>false</param-value>
         </init-param>

         <init-param>
            <param-name>viphost</param-name>
```

```
            <param-value>wcmserver.company.example</param-value>
         </init-param>
         <init-param>
            <param-name>vippport</param-name>
            <param-value>5008</param-value>
         </init-param>
         <init-param>
            <param-name>httpport</param-name>
            <param-value>5009</param-value>
         </init-param>
         <init-param>
            <param-name>secure</param-name>
            <param-value>false</param-value>
         </init-param>
         <init-param>
            <param-name>profile</param-name>
            <param-value>wcm</param-value>
         </init-param>
         <init-param>
            <param-name>loglevel</param-name>
            <param-value>0</param-value> <!-- 191 -->
         </init-param>
         <init-param>
            <param-name>realm</param-name>
            <param-value>WCM</param-value>
         </init-param>
         <init-param>
            <param-name>logdir</param-name>
            <param-value>d:/wcm/log</param-value>
         </init-param>
         <init-param>
            <param-name>logname</param-name>
            <param-value>filter_1</param-value>
         </init-param>
</filter>
-->

<!-- for IIS usage
      <init-param>
         <param-name>pattern1</param-name>
         <param-value>asp</param-value>
      </init-param>
      <init-param>
         <param-name>servlet1</param-name>
         <param-value>redirect</param-value>
      </init-param>
      <init-param>
         <param-name>redirect-url</param-name>
```

```
         <param-value>http://wcmserver.company.example/secret
            </param-value>
      </init-param>
-->

<!--
<filter-mapping>
      <filter-name>AccessFilter</filter-name>
      <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

Gemeinsame Parameter für das Secure Access-Servlet und den Secure Access-Filter

Im Folgenden werden die Einträge erläutert, die sowohl für das Servlet als auch für den Filter konfiguriert werden können.

Parameter `servlet-name` bzw. `filter-name`

Mithilfe dieses Parameters geben Sie an, ob das Servlet oder der Filter verwendet werden soll. Mögliche Einträge:

- Servlet für Secure Access

```
<servlet-name>AccessServlet</servlet-name>
<servlet-class>de.gauss.vip.vipsecure.AccessServlet
   </servlet-class>
```

- Filter für Secure Access

```
<filter-name>AccessFilter</filter-name>
<filter-class>de.gauss.vip.vipsecure.AccessFilter
   </filter-class>
```

Parameter `character-encoding`

Beispiel:

```
<init-param>
      <param-name>character-encoding</param-name>
      <param-value>UTF-8</param-value>
</init-param>
```

Mithilfe dieses Parameters können Sie das Encoding für die Übergabe der Secure Access-Parameter einstellen.

Wurde bei der Installation des in der JSP-Engine laufenden Content-Servers als Encoding für den Content-Client UTF-8 ausgewählt, dann muss auch für das Servlet bzw. den Filter von Secure Access `UTF-8` eingestellt werden. Alternativ können Sie `ISO-8859-1` für Latin-1-Encoding angeben. Wenn dieser Parameter nicht gesetzt ist, wird Latin-1-Encoding verwendet.

> **Hinweis:** Die Verwendung von UTF-8 (Unicode) muss konsistent für alle Komponenten von Livelink WCM Server konfiguriert werden. Bitte beachten Sie die Hinweise zur Verwendung von Unicode im Livelink WCM Server-Administratorhandbuch (Kapitel “Konzepte”).

Parameter `pathfrom` und `pathto`

Beispiel:

```
<init-param>
      <param-name>pathfrom</param-name>
      <param-value></param-value>
</init-param>
<init-param>
      <param-name>pathto</param-name>
      <param-value>d:/wcm/website</param-value>
</init-param>
```

Dies ist ein zusätzlicher Ersetzungsmechanismus für die Verwendung von Pfadangaben statt URLs.

- Für den Fall, dass der Parameter `usepath` den Wert `false` hat: Tragen Sie im Parameter `pathto` das Basisverzeichnis entsprechend der Konfiguration des HTTP-Servers ein. (Bei Apache entspricht dies dem Parameter `DocumentRoot` oder einem eventuell eingerichteten Alias; bei Tomcat entspricht dies dem Pfad zum Verzeichnis **\webapps**.) Der Parameter `pathfrom` sollte leer bleiben.
- Für den Fall, dass der Parameter `usepath` den Wert `true` hat: Falls Fehler bei der Pfadangabe auftreten – z.B. durch virtuelle Verzeichnisse – können Sie durch Angabe beider Parameter den ersten Teil der Pfadangabe korrigieren.

Parameter `usepath`

Beispiel:

```
<init-param>
      <param-name>usepath</param-name>
      <param-value>false</param-value>
</init-param>
```

Zeigt an, ob die Bearbeitung von Anfragen auf Grundlage von URLs oder umgesetzten Pfadangaben erfolgt. Mögliche Werte:

- `true`
  Es werden Pfadangaben statt URLs verwendet.
- `false`
  Es werden URLs verwendet.

Welche Option Sie hier einschalten, hängt davon ab, ob die JSP-Engine das Verwenden von Pfadangaben unterstützt. Ist dies für alle Objekttypen der Fall, können Sie hier `true` einstellen.

Server-Parameter (viphost, vippport, httpport, secure)

Beispiel:

```
<init-param>
      <param-name>viphost</param-name>
      <param-value>wcmserver.company.example</param-value>
</init-param>
<init-param>
      <param-name>vippport</param-name>
      <param-value>5008</param-value>
</init-param>
<init-param>
      <param-name>httpport</param-name>
      <param-value>5009</param-value>
</init-param>
<init-param>
      <param-name>secure</param-name>
      <param-value>false</param-value>
</init-param>
```

Mithilfe dieser Parameter spezifizieren Sie die Verbindung zu einem Server. Geben Sie den Namen des Hostrechners und die Ports an, über die der Server erreicht werden kann. Mithilfe des Parameters `secure` wird angegeben, ob die Verbindung über SSL laufen soll.

> **Hinweis:** Diese Angaben müssen mit der Konfiguration im Admin-Client übereinstimmen. Die Parameter für die Verbindung zum Server werden in den Einstellungen des WCM-Pools des Servers festgelegt.

Parameter profile

Beispiel:

```
<init-param>
      <param-name>profile</param-name>
      <param-value>wcm</param-value>
</init-param>
```

Dieser Parameter enthält den Namen des Webservers, wie er im Admin-Client in den Einstellungen des Servers auf dem Register *Secure Access* angegeben wurde (siehe Abschnitt “Secure Access in den Server-Einstellungen aktivieren” auf Seite 205).

Parameter für das Secure Access-Protokoll (`loglevel`, `logdir`, `logname`)

Die Meldungen von Secure Access werden standardmäßig in der Datei **vipsecure_servlet.log** bzw. **vipsecure_filter.log** im Verzeichnis **{WCM-Installationsverzeichnis}\log** protokolliert. Das Protokoll enthält alle Anfragen des Webservers an Livelink WCM Server und die entsprechenden Antworten. Mithilfe der Log-Parameter steuern Sie die Protokollierung.

Hinweise:

Die Zugriffsrechte auf das Verzeichnis, in das die Protokolldateien geschrieben werden, müssen sowohl unter Windows als auch unter UNIX so eingestellt werden, dass der Benutzer, unter dessen Kennung der Webserver läuft, Schreib- und Leserechte besitzt (siehe Abschnitt “Schreibrechte für die Verzeichnisse von Livelink WCM Server” auf Seite 126).

Zusätzlich zu diesem Protokoll ist es möglich, die Anfragen und Antworten zwischen Secure Access und dem entsprechenden Server in der Protokolldatei des Servers zu protokollieren. Dieses Protokoll aktivieren Sie mithilfe des Parameters `-Dvip.vipsecure.debug=true` in den Startskripten der Server (siehe Tabelle 19 “Parameter in den Startskripten der Server” auf Seite 166).

- Parameter `loglevel`

  Beispiel:

```
<init-param>
<param-name>loglevel</param-name>
   <param-value>24</param-value>
</init-param>
```

Der Loglevel steuert den Detaillierungsgrad bzw. den Umfang der Protokollierung von Secure Access. Der Eintrag ist optional. Die folgenden Loglevels können festgelegt werden:

Tabelle 21 – Loglevels von Secure Access

Loglevel	Erläuterung
8	alle Fehlermeldungen
16	alle Warnmeldungen
32	alle Informationsmeldungen, z.B. über Anfragen, und dazugehörige Antworten
64	ausführliche Informationen
0	nichts

Um verschiedene Loglevel zu kombinieren, addieren Sie einfach die Zahlen. Wenn z.B. alle Meldungen mit den Levels “Warnung” (16) und “Fehler” (8) im Protokoll enthalten sein sollen, setzen Sie den Wert `loglevel` auf 24. Standardwert ist 0. Ein hoher Wert wie 191 oder 255 sollte nur in Ausnahmefällen, z.B. zur Fehlersuche, verwendet werden.

- Parameter `logdir`

  Beispiel:

```
<init-param>
   <param-name>logdir</param-name>
   <param-value>d:/wcm/log</param-value>
</init-param>
```

  Verzeichnis, in dem das Protokoll mit den Meldungen von Secure Access gespeichert wird

- Parameter `logname`

  Beispiel:

```
<init-param>
   <param-name>logname</param-name>
   <param-value>servlet-1</param-value>
</init-param>
```

  Mithilfe dieses Parameters können Sie einen Zusatz für den Standardnamen des Secure Access-Protokolls definieren. Mit dem im Beispiel angegeben Namen würde das Protokoll **vipsecure_servlet-1.log** heißen.

  Dieser Parameter ist optional. Die Angabe eines Namenszusatzes kann z. B. sinnvoll sein, wenn in einer JSP-Engine (bzw. einem Webserver) mehrere Secure Access-Servlets bzw. Secure Access-Filter laufen. Auf diese Weise können die Meldungen der verschiedenen Servlets bzw. Filter in unterschiedlichen Dateien protokolliert werden.

Parameter `realm`

Beispiel:

```
<init-param>
      <param-name>realm</param-name>
      <param-value>WCM</param-value>
</init-param>
```

Der hier angegebene Text wird im Anmeldedialog des Browsers angezeigt, wenn sich ein Benutzer für den Zugriff auf ein geschütztes Verzeichnis authentifiziert.

Parameter `redirect-dir` und `redirect-url`

Beispiel:

```
<init-param>
      <param-name>redirect-dir</param-name>
      <param-value>d:/wcm/website/secret</param-value>
</init-param>
<init-param>
      <param-name>redirect-url</param-name>
      <param-value>http://wcmserver.company.example/secret</param-value>
</init-param>

<init-param>
      <param-name>pattern1</param-name>
      <param-value>asp</param-value>
</init-param>
<init-param>
      <param-name>servlet1</param-name>
      <param-value>redirect</param-value>
</init-param>
```

Mithilfe dieser Parameter geben Sie ein Verzeichnis und eine URL für die spezielle Umleitung – z. B. von ASP-Dateien – an. Die Parameter `redirect-dir` und `redirect-url` werden nur genutzt, wenn für ein Pattern (z. B. `asp`) das Servlet “redirect” angegeben wird.

Achtung!

Die angegebene `redirect-url` darf nicht von Secure Access überwacht werden! Für Resin und IIS muss hierzu z.B. in der Datei **resin.conf** das Mapping für das Plugin explizit mithilfe eines entsprechenden URL-Mappings ausgeschaltet werden `<servlet-mapping url-pattern='/secret/*' servlet-name='plugin_ignore'/>`.

Die URL darf außerdem von außen nicht direkt zugreifbar sein. Konfigurieren Sie Ihren Webserver entsprechend.

- `redirect-dir` (optional) – Die Dateien (deren Typ mithilfe des Parameters `patternX` spezifiziert wurde) werden mit zufälligen Dateinamen in dieses Verzeichnis kopiert, damit sie dort z.B. von der DLL für ASP-Seiten bearbeitet werden können.
- `redirect-url` – URL für den Zugriff auf dieses Verzeichnis. Wurde ein Verzeichnis im Parameter `redirect-dir` angegeben, dann muss der HTTP-Server so konfiguriert werden, dass die angegebene URL dieses Verzeichnis abbildet. Wurde im Parameter `redirect-dir` kein Verzeichnis angegeben, dann muss der HTTP-Server so konfiguriert werden, dass diese URL die Originalverzeichnisse der Dateien abbildet. In diesem Fall werden die Dateien in den Originalverzeichnissen bearbeitet.
- `pattern` und `servlet` – siehe Abschnitt “Parameter `pattern` und `servlet`” auf Seite 222

Parameter `url-pattern`

Beispiel:

```
<servlet-mapping>
      <servlet-name>AccessServlet</servlet-name>
      <url-pattern>/*</url-pattern>
</servlet-mapping>

<filter-mapping>
      <filter-name>AccessFilter</filter-name>
      <url-pattern>/*</url-pattern>
</filter-mapping>
```

Mithilfe dieses Parameters geben Sie die URLs an, die durch Secure Access geschützt werden sollen. Folgende Werte sind möglich:

- `/*`
  Alle URLs, die über diesen HTTP-Server erreicht werden können
- `/{Name des Deploymentsystemverzeichnisses}/*`
  Alle URLs, die auf die Verzeichnisse verweisen, die im Admin-Client als Pfade für Secure Access konfiguriert wurden. Wenn Sie im Admin-Client mehrere Pfade für Secure Access definiert haben, machen Sie für jedes Verzeichnis einen separaten Eintrag.
- `'*.xyz'`
  Alle URLs, die auf Dateien mit der angegebenen Dateiendung verweisen

Hinweise:

Die verschiedenen Werte können nicht miteinander kombiniert werden.

Das URL-Mapping greift nur für Anfragen, die auch an die JSP-Engine weitergeleitet werden. Insbesondere wenn der HTTP-Server über ein Plugin mit der JSP-Engine kommuniziert, werden Filter-Mappings i.A. vom Plugin ignoriert, sodass die JSP-Engine (und damit Secure Access) diese Anfragen nicht sieht. Für diese Fälle müssen Sie zusätzlich das Plugin so konfigurieren, dass entsprechende Anfragen an die JSP-Engine weitergeleitet werden.

Zusätzliche Parameter für das Secure Access-Servlet

Wenn Sie das Secure Access-Servlet verwenden, müssen außerdem Mappings für alle anderen Servlets vorgenommen werden, die Sie bereits in der JSP-Engine konfiguriert haben. Wenn das Secure Access-Servlet alle Dateien in einem geschützten Verzeichnis bearbeitet (Parameter `<servlet-mapping url-pattern='/{Name des Deploymentsystemverzeichnisses}/*'`), dann müssen einige Dateitypen anschließend an andere Servlets weitergeleitet werden.

Warnung!

Herstellerspezifische Servlets wie z.B. das `com.caucho.server.http.FileServlet` können über eigene Cache-Mechanismen verfügen, die die Sicherheitsmechanismen des Secure Access-Servlets umgehen.

Derartige Servlets dürfen nicht als `servletX` in den unten beschriebenen Pattern-Servlet-Paaren konfiguriert werden. Ist ihre Verwendung unumgänglich, muss der Cache-Mechanismus (bei Resin z.B. mit `<cache enable='false'/>`) deaktiviert werden. Ansonsten kann es vorkommen, dass geschützte Seiten über den Cache auch für nicht autorisierte Benutzer verfügbar sind.

Im Folgenden werden die Einträge erläutert, die für das Servlet-Mapping vorgenommen werden müssen.

Parameter `pattern` und `servlet`

Beispiel:

```
<init-param>
      <param-name>pattern1</param-name>
      <param-value>jsp</param-value>
</init-param>
<init-param>
      <param-name>servlet1</param-name>
      <param-value>resin-jsp</param-value>
</init-param>
```

Geben Sie im Parameter `patternX` die Endung der Dateien (ohne Punkt) an, die nach der Bearbeitung durch Secure Access an ein anderes Servlet weitergeleitet werden sollen.

Mögliche Werte für `servletX`:

- `'{Name des Servlets}'`
  der Name des Servlets. Der Wert dieses Parameters ist abhängig von der verwendeten JSP-Engine.

  Für Resin wird der Name des JSP-Servlets in der Datei **app-default.xml** im Verzeichnis **{Resin-Installationsverzeichnis}\conf** festgelegt. Bis zur Version 3.0.8 von Resin ist der Standardname “jsp”, in höheren Version “resin-jsp”.

- `'redirect'`
  Für die Weiterleitung sollen ein gesondertes Verzeichnis und spezielle URLs verwendet werden. Dies ist z.B. für die Verarbeitung von ASP-Seiten erforderlich, die bei IIS mit einer speziellen DLL erfolgt. Verzeichnis und URL werden mithilfe der Parameter `redirect-dir` und `redirect-url` angegeben.

Konfigurieren Sie weitere Pattern-Servlet-Paare entsprechend Ihren Anforderungen.

Parameter `directory-servlet`

Beispiel:

```
<init-param>
      <param-name>directory-servlet</param-name>
      <param-value>com.caucho.server.http.DirectoryServlet</param-value>
</init-param>
```

Wenn Sie diesen Parameter konfigurieren, werden bei der Darstellung eines Verzeichnisses im Browser wie gewohnt die dazugehörigen Unterverzeichnisse angezeigt.

Parameter `setcontentlength`

Beispiel:

```
<init-param>
      <param-name>setcontentlength</param-name>
      <param-value>true</param-value>
</init-param>
```

Mithilfe dieses Parameters geben Sie an, ob die Content-Length (die Größe des vom Server zurückgegebenen Objekts) durch Secure Access gesetzt werden soll. Das Setzen dieses Parameters ist optional, der Standardwert ist `true`.

> **Hinweis:** Wenn Sie den Application-Server IBM WebSphere nutzen, setzen Sie diesen Parameter auf `false`. IBM WebSphere bestimmt die Content-Length selbst.

Parameter `welcome-file-list`

Beispiel:

```
<init-param>
      <param-name>welcome-file-list</param-name>
      <param-value>index.htm,index.html,index.jsp</param-value>
</init-param>
```

Mithilfe dieses Parameters können Sie eine Liste von Dateien angeben, die Secure Access bei der Bearbeitung eines Requests für ein Verzeichnis berücksichtigen soll. Gehört die zu bearbeitende URL zu einem Verzeichnis, so prüft Secure Access, ob eine in diesem Parameter spezifizierte Datei in dem Verzeichnis vorhanden ist und liefert den Inhalt der ersten auf diese Weise ermittelten Datei zurück.

HTTP-Requests für geschützte Seiten nachbearbeiten

Im Verzeichnis **{WCM-Installationsverzeichnis}\examples\vipsecure** befinden sich die Java-Klassen `IPTranslator` und `DomainTranslator`. Mithilfe dieser Klassen können die HTTP-Requests geschützter Seiten nachbearbeitet werden, bevor sie an das WCM-System weitergeleitet werden. Auf diese Weise kann z.B. im Request der Benutzername entsprechend der IP-Adresse gesetzt werden, sodass auf Grundlage dieser Information eine automatische Authentifizierung vorgenommen werden kann. Ein weiteres Anwendungsbeispiel ist die Abtrennung der in Benutzerkennungen enthaltenen Domänennamen. Die genaue Art und Weise der Nachbearbeitung von Anforderungen erfolgt über eine Anpassung der Klasse `IPTranslator` bzw. `DomainTranslator`.

Nach dem Einbinden der Klassen in die JSP-Engine werden die Klassen bei jeder Anforderung einer geschützten Seite aufgerufen. Aus der Anforderung werden Informationen wie der absolute Pfad der angeforderten Seite, Benutzer, Passwort, IP-Adresse und Context-ID herausgelesen. Diese Informationen können anschließend bearbeitet werden.

So konfigurieren Sie die Nachbearbeitung von HTTP-Requests:

1. Passen Sie die mitgelieferte Java-Klasse `IPTranslator` bzw. `DomainTranslator` Ihren Erfordernissen an.

   Informationen dazu erhalten Sie in den Kommentaren der Klassen.

2. Übersetzen Sie die geänderte Java-Klasse.
3. Machen Sie die Klassen für die JSP-Engine verfügbar, indem Sie sie in den Klassenpfad der JSP-Engine eintragen.
4. Fügen Sie den folgenden Parameter der Konfiguration des Secure Access-Servlets bzw. Filters hinzu:

```
<init-param>
       <param-name>translator</param-name>
       <param-value>{Name des Packages}.{Klassenname}</param-value>
</init-param>
```

5. Starten Sie die JSP-Engine neu.

KAPITEL 6

Upgrade von Livelink WCM Server

Die Upgrade-Option im Installationsprogramm ermöglicht es Ihnen, eine bestehende WCM-Installation in einen höheren Versionsstand zu überführen und die existierenden Website-Daten an die neue Datenstruktur anzupassen.

In diesem Kapitel werden die folgenden Themen behandelt:

- Upgrade über die grafische Oberfläche (siehe folgenden Abschnitt)
- Upgrade über die Konsole (siehe Abschnitt 6.2 “Upgrade über die Konsole” auf Seite 236)
- Nacharbeiten nach Durchführung eines Upgrades (siehe Abschnitt 6.3 “Notwendige Nacharbeiten nach dem Upgrade” auf Seite 240)

6.1 Upgrade über die grafische Oberfläche

Das Upgrade von Livelink WCM Server wird in zwei Schritten durchgeführt:

1. Anpassen der Konfiguration und Kopieren aller notwendigen Dateien (siehe folgenden Abschnitt)
2. Anpassen der Tabellenstruktur und -inhalte in der verwendeten Datenbank (siehe Abschnitt “Upgrade der Datenhaltung durchführen” auf Seite 231)

Wenn Sie die Datenbank für die Speicherung der Website-Daten wechseln möchten, exportieren Sie zunächst mithilfe des Export/Import-Tools die Websites aus dem WCM-System. Führen Sie anschließend das Upgrade der Version durch. Legen Sie dann einen Pool für die neue Datenbank an, und importieren Sie die Website unter Angabe dieses Pools in das upgegradete WCM-System.

Hinweise:

Bitte beachten Sie, dass Sie eine Website nur löschen können, wenn die Version der Website der Version des WCM-Systems entspricht.

Hinweise zur Verwendung des Export/Import-Tools finden Sie im Livelink WCM Server-Administratorhandbuch (Kapitel “Websites verwalten”).

Upgrade der Version durchführen

Hinweise

- Folgende Reihenfolge ist beim Upgrade der einzelnen Komponenten eines verteilten WCM-Systems zu berücksichtigen: Zuerst muss für den Master-Admin-Server, dann für eventuell vorhandene Proxy-Admin-Server das Upgrade durchgeführt werden. Anschließend werden der Master-Content-Server und vorhandene Proxy-Server upgegradet.
- In einem verteilten WCM-System muss für jedes Installationsverzeichnis, in dem sich Komponenten des WCM-Systems befinden, ein separates Upgrade durchgeführt werden. Dabei werden immer alle Komponenten, die sich in dem Verzeichnis befinden, gleichzeitig upgegradet.
- Vor der Durchführung eines Upgrades müssen die Datenbestände des WCM-Systems gesichert werden. Ausführliche Informationen

zum Backup finden Sie im Livelink WCM Server-Administratorhandbuch.

Wenn Sie das RDBMS Oracle verwenden, aktualisieren Sie außerdem die Statistiken.

Wenn Sie eine LDAP-basierte Benutzerverwaltung verwenden, führen Sie für den LDAP-Verzeichnisdienst eine Datensicherung durch.

- Content-Server können nur auf Website-Daten zugreifen, deren Datenstruktur der eigenen WCM-Version entspricht. Beispielsweise kann ein Server mit der Version 9.2.1 keine Websites hochfahren, deren Datenhaltung bereits an die Version 9.5 angepasst wurde.

Voraussetzungen

- Das WCM-System, für das ein Upgrade durchgeführt werden soll, hat die Version 8.1.1 oder höher.
- Die Server, für die das Upgrade durchgeführt werden soll, befinden sich im Runlevel “Server nicht erreichbar”.
- Es muss sichergestellt sein, dass keine Prozesse auf Dateien des installierten WCM-Systems zugreifen.
- Das Upgrade basiert auf dem Kopieren von Verzeichnissen. Im Dateisystem wird deshalb für die Durchführung des Upgrades zusätzlicher freier Speicherplatz benötigt.

Vorgehensweise

So führen Sie ein Upgrade der Version mithilfe der grafischen Oberfläche des Installationsprogramms durch:

1. Starten Sie das Installationsprogramm (siehe Abschnitt “Installation starten” auf Seite 73), und wählen Sie das Installationsverzeichnis des bestehenden WCM-Systems aus.

2. Aktivieren Sie im Dialog *Typ der Installation* das Optionsfeld *Upgrade der Version*, und klicken Sie auf die Schaltfläche *Weiter*.

   Im Dialog *Informationen zum Upgrade* werden Ihnen die aktuelle Version des WCM-Systems und die zukünftige Version (nach erfolgreich durchgeführtem Upgrade) angezeigt.

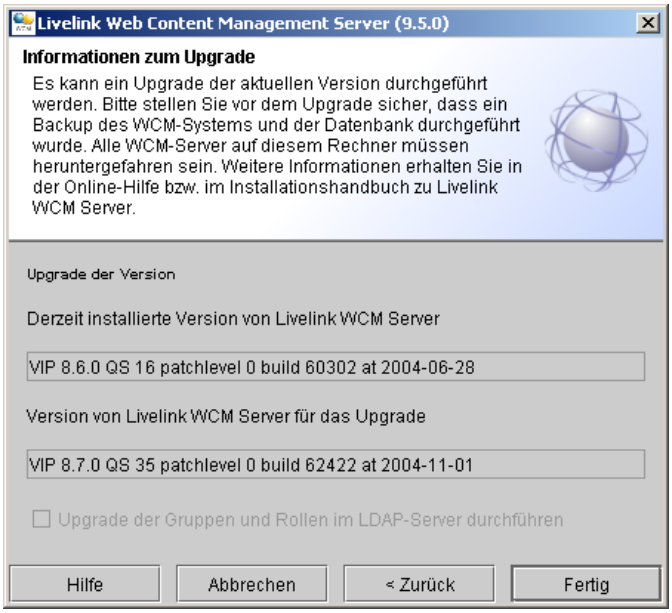

Livelink Web Content Management Server (9.5.0)
Informationen zum Upgrade
Es kann ein Upgrade der aktuellen Version durchgeführt werden. Bitte stellen Sie vor dem Upgrade sicher, dass ein Backup des WCM-Systems und der Datenbank durchgeführt wurde. Alle WCM-Server auf diesem Rechner müssen heruntergefahren sein. Weitere Informationen erhalten Sie in der Online-Hilfe bzw. im Installationshandbuch zu Livelink WCM Server.
Upgrade der Version
Derzeit installierte Version von Livelink WCM Server
VIP 8.6.0 QS 16 patchlevel 0 build 60302 at 2004-06-28
Version von Livelink WCM Server für das Upgrade
VIP 8.7.0 QS 35 patchlevel 0 build 62422 at 2004-11-01
Upgrade der Gruppen und Rollen im LDAP-Server durchführen
Hilfe
Abbrechen
< Zurück
Fertig

Abb. 25 – Upgrade der Version durchführen

3. Wenn Sie in der Vergangenheit die Version 8.1 mit einer LDAP-basierten Benutzerverwaltung eingesetzt haben, muss unter Umständen die LDAP-Datenstruktur angepasst werden. Aktivieren Sie dazu das Kontrollkästchen *Upgrade der Gruppen und Rollen im LDAP-Server durchführen*.
4. Klicken Sie auf die Schaltfläche *Fertig*.

Für alle Server, die sich in dem angegebenen Verzeichnis befinden, wird nun gleichzeitig das Upgrade durchgeführt.

Zunächst erstellt das Upgrade eine Sicherungskopie des Verzeichnisses **{WCM-Installationsverzeichnis}\config**. Anschließend werden die Konfigurationsdateien an die Version 9.5 angepasst. Der Fortschritt wird auf der Konsole angezeigt und in der Datei **{WCM-Installationsverzeichnis}\installation\ installation.log** protokolliert.

Nachdem die Konfiguration angepasst wurde, werden einige Dateien kopiert. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

5. Wurde das Upgrade für einen Administrationsserver durchgeführt, starten Sie diesen, und spielen Sie die Lizenz für die Version 9.5 ein (siehe Abschnitt 4.5 “Lizenz erneuern” auf Seite 124).

Upgrade der Datenhaltung durchführen

Hinweise

- Durch das Upgrade werden die Datenbanktabellen des WCM-Systems verändert. Führen Sie deshalb vor Beginn des Upgrade-Prozesses unbedingt ein manuelles Backup der Datenbank (Tabellen, Prozeduren, Packages, Trigger) durch.
- Wenn Sie ein verteiltes WCM-System mit Proxy-Content-Server und separater Datenhaltung verwenden, können gegebenenfalls nicht alle Proxy-Datenhaltungen zentral über den Master-Admin-Server upgegradet werden. Führen Sie in dem Fall das Upgrade der Datenhaltung auf den entsprechenden Servern durch.

Voraussetzungen

- Die Datenstruktur der Website, für die ein Upgrade durchgeführt werden soll, entspricht der Version 8.1.1 oder höher.
- Das Upgrade der Version muss mindestens für den Master-Admin- und den Master-Content-Server erfolgreich durchgeführt worden sein.
- Alle Server, die Datenhaltungen verwenden, für die ein Upgrade durchgeführt werden soll, müssen sich im Runlevel “Server nicht erreichbar” befinden.
- Der zugeordnete Admin-Server muss sich im Runlevel “Server läuft” befinden.
- Der Datenbankbenutzer muss für das Upgrade des WCM-Systems über dieselben Rechte und Zuordnungen verfügen wie für die Installation (siehe Abschnitt “Berechtigungen und Zuordnungen des Benutzers” auf Seite 28).
- Im Tablespace der verwendeten Datenbank muss ausreichend freier Speicherplatz vorhanden sein. Empfohlen werden mindestens 20 Prozent freier Tablespace.

Vorgehensweise

So führen Sie ein Upgrade der Datenhaltung mithilfe der grafischen Oberfläche des Installationsprogramms durch:

1. Starten Sie das Installationsprogramm (siehe Abschnitt “Installation starten” auf Seite 73), und wählen Sie das Installationsverzeichnis des bestehenden WCM-Systems aus.
2. Aktivieren Sie im Dialog *Typ der Installation* das Optionsfeld *Upgrade der Datenhaltung*, und klicken Sie auf die Schaltfläche *Weiter*.
3. Wenn Sie das Upgrade von einem Hostrechner starten, auf dem kein Admin-Server installiert ist, muss eine Verbindung zum Admin-Server hergestellt werden. Geben Sie im Dialog *Admin-Server* die

Parameter des zuständigen Admin-Servers an, damit eine Verbindung zu diesem Server aufgebaut werden kann.

Sie können diese Parameter im Admin-Client über *Konfiguration* → *Pools* → *WCM* → *{Pool des Admin-Servers}* überprüfen.

4. Klicken Sie auf die Schaltfläche *Testen*.
5. Sie müssen sich nun beim Admin-Server anmelden. Geben Sie die Benutzerkennung und das Passwort des zuständigen Administrators ein.
6. Bestätigen Sie den Dialog *Admin-Server* durch Klicken auf die Schaltfläche *Weiter*.
7. Das Upgrade versucht, alle in der Konfiguration existierenden JDBC-Pools zu erreichen. Dieser Vorgang ist unabhängig von der Zuordnung der Pools zu Proxy-Servern.

   Um die Verbindungen zur Datenbank herzustellen, greift das Upgrade auf das Verzeichnis **{WCM-Installationsverzeichnis}\external_lib** zu und sucht in den dort befindlichen JAR- bzw. ZIP-Dateien nach JDBC-Treibern.

   Ist der Verbindungsaufbau erfolgreich, wird die Version der vorhandenen Datenstrukturen ausgelesen. Wenn die Verbindung nicht aufgebaut werden kann, wird dies für den entsprechenden Pool unter *Version oder Hinweis* vermerkt.

   Im folgenden Dialog werden Ihnen die Datenhaltungen angezeigt, für die ein Upgrade durchgeführt werden kann.

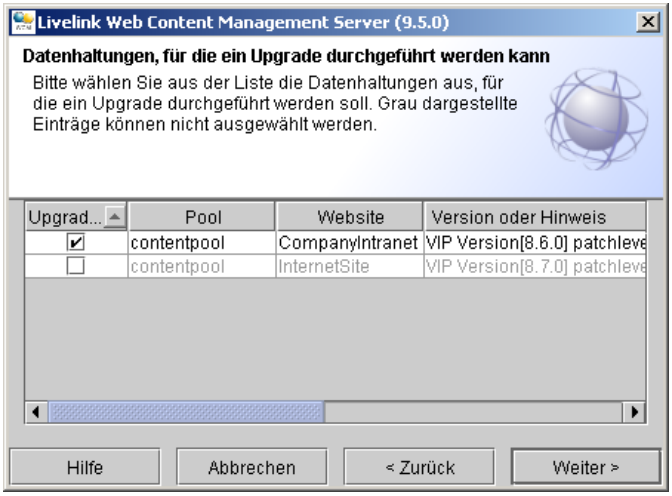


Abb. 26 – Upgrade der Datenhaltung durchführen

8. Aktivieren Sie das Auswahlkästchen der Kombination aus Pool und Website, für die das Upgrade durchgeführt werden soll.

   Im Dialog *Ausgewählte Datenhaltungen* wird Ihnen eine Übersicht der Datenhaltungen angezeigt, für die das Upgrade durchgeführt wird.

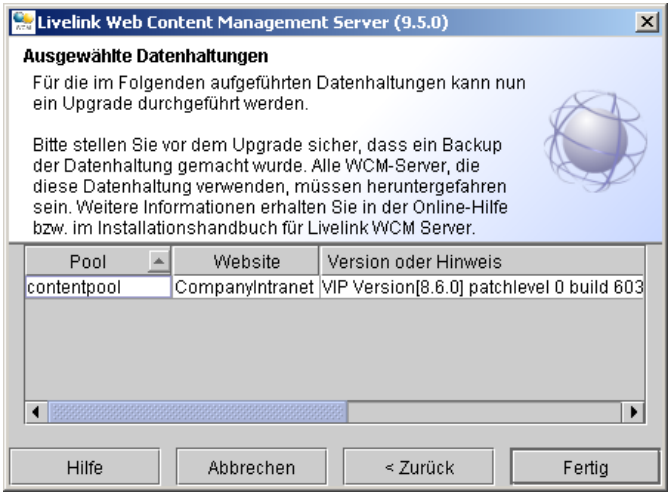

Livelink Web Content Management Server (9.5.0)
Ausgewählte Datenhaltungen
Für die im Folgenden aufgeführten Datenhaltungen kann nun ein Upgrade durchgeführt werden.
Bitte stellen Sie vor dem Upgrade sicher, dass ein Backup der Datenhaltung gemacht wurde. Alle WCM-Server, die diese Datenhaltung verwenden, müssen heruntergefahren sein. Weitere Informationen erhalten Sie in der Online-Hilfe bzw. im Installationshandbuch für Livelink WCM Server.
Pool
Website
Version oder Hinweis
contentpool
CompanyIntranet
VIP Version[8.6.0] patchlevel 0 build 603
Hilfe
Abbrechen
< Zurück
Fertig

Abb. 27 – Für das Upgrade ausgewählte Datenhaltungen

9. Klicken Sie auf die Schaltfläche *Fertig*.

   Nachdem die Website an die Datenstruktur der Version 9.5 angepasst wurde, kann der entsprechende Content-Server neu gestartet werden. Die Website ist jetzt wieder zugreifbar.

Achtung! Sollten während des Upgrades der Datenhaltung Fehler auftreten, so können die bereits vorgenommenen Änderungen nicht mehr rückgängig gemacht werden. Spielen Sie in dem Fall das Datenbank-Backup ein.

6.2 Upgrade über die Konsole

Alternativ zum Upgrade über die grafische Oberfläche kann das WCM-System auch mithilfe der Konsole upgegradet werden. Die einzelnen Schritte und erforderlichen Nacharbeiten entsprechen dem Upgrade über die grafische Oberfläche.

Upgrade der Version über die Konsole steuern

Hinweise:

Bitte beachten Sie auch die Hinweise und Voraussetzungen im Abschnitt “Upgrade der Version durchführen” auf Seite 228.

Informationen zum Starten des Upgrades über die Konsole erhalten Sie im Abschnitt “Installation über die Konsole starten” auf Seite 160.

Um im ersten Schritt das Upgrade der Version durchzuführen, müssen Sie in der Datei **defaults.xml** (befindet sich im Verzeichnis **\installation** der WCM-CD) Anpassungen vornehmen. Dies betrifft die folgenden Abschnitte; die Angaben für die übrigen Abschnitte werden automatisch aus dem installierten System ausgelesen.

Angaben im Abschnitt `<common>`

Dieser Abschnitt muss vollständig ausgefüllt sein (siehe Abschnitt “Angaben im Abschnitt <common>” auf Seite 140). Insbesondere muss der Eintrag `<install_action>` auf den Werte `none` gesetzt werden.

Angaben im Abschnitt `<rdbms>`

In diesem Abschnitt muss der Eintrag `<check>` auf den Wert `false` gesetzt werden.

Angaben im Abschnitt <update_vip>

Dieser Abschnitt muss ausgefüllt sein.

```
<update_vip>
      <update_ldap>false</update_ldap>
      <install_action>update</install_action>
</update_vip>
```

Die folgende Tabelle erläutert die einzelnen Einträge.

Tabelle 22 – Angaben im Abschnitt <update_vip>

Eintrag in der XML-Datei	Erläuterung
`<update_ldap>false</update_ldap>`	Wenn Sie in der Vergangenheit die Version 8.1 mit einer LDAP-basierten Benutzerverwaltung eingesetzt haben, muss unter Umständen die LDAP-Datenstruktur angepasst werden. Mögliche Werte: `true` (Anpassen der LDAP-Datenstruktur), `false` (kein Anpassen der LDAP-Datenstruktur)
`<install_action>update</install_action>`	Upgrade-Option für das WCM-System Mögliche Werte: `update` (Upgrade der Version durchführen), `none` (kein Upgrade der Version durchführen)

Die Ausgabe auf der Konsole enthält die Information über die aktuelle und zukünftige (nach dem Upgrade) Version von Livelink WCM Server.

```
------------------------------------------------------------------
start version update
current installed version VIP 8.6.0 QS 16 patchlevel 0 build 60302 at
2004-06-28
version to install VIP 8.7.0 QS 35 patchlevel 0 build 62422 at 2004-11-01
------------------------------------------------------------------
Created directory: D:\wcm|backup_1099398160677
```

```
Xcopy: D:\wcm|config to: D:\wcm|backup_10993981606
update started
update : current master id is 79
update config/server.xml : step 80 started
update config/server.xml : step 80 finished
update : current master id is 80
...
```

Upgrade der Datenhaltung durchführen

Hinweise:

Bitte beachten Sie auch die Hinweise und Voraussetzungen im Abschnitt “Upgrade der Datenhaltung durchführen” auf Seite 231.

Informationen zum Starten des Upgrades über die Konsole erhalten Sie im Abschnitt “Installation über die Konsole starten” auf Seite 160.

Um im zweiten Schritt das Upgrade der Datenhaltung durchzuführen, müssen Sie in der Datei **defaults.xml** (befindet sich im Verzeichnis **\installation** der WCM-CD) Anpassungen vornehmen. Dies betrifft die folgenden Abschnitte; die Angaben für die übrigen Abschnitte werden automatisch aus dem installierten System ausgelesen.

Angaben im Abschnitt <admin>

Dieser Abschnitt muss vollständig ausgefüllt sein (siehe Abschnitt “Angaben im Abschnitt <admin>” auf Seite 142). Insbesondere muss der Parameter <install_action> auf den Wert none gesetzt werden.

Angaben im Abschnitt <update_vip>

In diesem Abschnitt muss der Eintrag <install_action> auf den Wert none gesetzt werden.

Angaben im Abschnitt <update_rdbms>

Dieser Abschnitt muss ausgefüllt sein.

```
<update_rdbms>
      <pool name="contentpool">
         <website>InternetSite</website>
      </pool>
      <install_action>update</install_action>
</update_rdbms>
```

Die folgende Tabelle erläutert die einzelnen Einträge.

Tabelle 23 – Angaben im Abschnitt <update_rdbms>

Eintrag in der XML-Datei	Erläuterung
<pool name="contentpool">	Name des JDBC-Pools für die Datenbankverbindung. Über diese Datenbankverbindung werden die WCM-Objekte der im Eintrag <website> angegebenen Website vom Master-Content-Server gespeichert.
<website>InternetSite</website>	Name der Website, die den im Eintrag <pool name> angegebenen JDBC-Pool verwendet und für die das Upgrade durchgeführt werden soll
<install_action>update</install_action>	Upgrade-Option für die Datenhaltung Mögliche Werte: update (Upgrade der Datenhaltung durchführen), none (kein Upgrade der Datenhaltung durchführen)

6.3 Notwendige Nacharbeiten nach dem Upgrade

Webanwendungen

Für alle Server, die im Application-Server als Webanwendung eingebunden sind, müssen nach dem Upgrade über den Admin-Client neue WAR-Dateien erzeugt werden (Informationen hierzu finden Sie im Livelink WCM Server-Administratorhandbuch).

Um die neu erzeugten WAR-Dateien auf dem Application-Server zu verteilen, gibt es zwei Möglichkeiten:

- mithilfe der Funktionalität des jeweiligen Application-Servers. Dabei ist zu beachten, dass einige Application-Server vor dem Neuverteilen der Webanwendung das Verzeichnis der Webanwendung löschen. In diesem Fall ist es erforderlich, die Deploymentsysteme neu anzulegen.
- durch Entpacken der WAR-Datei und Kopieren der entpackten Dateien in das vorhandene Verzeichnis der Webanwendung. Änderungen, die zuvor in der Datei **web.xml** vorgenommen wurden, müssen anschließend erneut gemacht werden.

Startskripte der Server

Nach einem erfolgreichen Upgrade müssen die servereigenen Startskripte in folgender Hinsicht manuell angepasst werden:

- Verwendung eines aktuelleren Java 2 SDK
- Einfügen zusätzlicher Kopierkommandos

  Die Kopierkommandos stellen sicher, dass Dateien, die sich im Verzeichnis **{WCM-Installationsverzeichnis}\latestpatch** eines Servers befinden, vor dem Start des Servers in dessen Verzeichnis **\lib** kopiert werden. Dies ermöglicht zu einem späteren Zeitpunkt eine einfache Installation von Service-Packs.

Für ein **Windows**-basiertes System müssen vor der Zeile

```
call "{WCM-Installationsverzeichnis}\setClasspath.bat"
```

folgende Zeilen eingefügt werden:

```
REM copy latest patch files
java -cp .\lib\vipcore.jar de.gauss.io.FileCopy .\latestpatch\
                                                        .\lib jar
```

Handelt es sich um einen Admin-Server, müssen folgende Zeilen eingefügt werden:

```
REM copy latest patch files
java -cp .\lib\vipcore.jar de.gauss.io.FileCopy .\latestpatch\
                                                        .\lib jar
java -cp .\lib\vipcore.jar de.gauss.io.FileCopy .\latestpatch\
                                                  .\admin\lib jar
```

Für ein **UNIX**-basiertes System müssen nach der Überprüfung, ob der WCM-Prozess als Root gestartet wurde, folgende Zeilen eingefügt werden:

```
for i in `ls ./lib/` ;do
   cp ./latestpatch/$i ./lib/$i 2>deleteme.txt
done
if [ -f deleteme.txt ]
then rm deleteme.txt
fi
```

Hinweis: Soll ein Content-Server gestartet werden, für den kein Startskript erstellt wurde, können Sie entweder ein vorhandenes Startkript kopieren und den Servernamen anpassen. Oder Sie verwenden das Skript **startserver.bat** und geben als Parameter den Namen des zu startenden Servers an.

RDMBS Oracle

Nach einem erfolgreichen Upgrade von Oracle-Datenbanktabellen sollten die Statistiken aktualisiert werden.

ANHANG A

Produktspezifische Hinweise für LDAP-Verzeichnisdienste

Dieser Anhang beschreibt die Besonderheiten, die bei der Vorbereitung der folgenden LDAP-Verzeichnisdienste für Livelink WCM Server zu beachten sind:

- Microsoft Active Directory, siehe folgenden Abschnitt
- Novell eDirectory Server, siehe Abschnitt “Novell eDirectory (NDS)” auf Seite 252
- Sun ONE Directory Server, siehe Abschnitt “Sun ONE Directory Server” auf Seite 257
- OpenLDAP, siehe Abschnitt “OpenLDAP” auf Seite 261

Welche Vorbereitungen Sie treffen müssen, um einen LDAP-Verzeichnisdienst mit Livelink WCM Server zu nutzen, erfahren Sie in Kapitel 3 “LDAP-Verzeichnisdienst einrichten”.

A.1 Microsoft Active Directory

Beim Verzeichnisdienst Microsoft Active Directory sind folgende Besonderheiten zu beachten.

Objektklassen

Die Objektklasse `vip` muss als abstrakte Basisklasse aller WCM-spezifischen Objektklassen angelegt werden (Active Directory-Objektklassentyp = ”Zusammenfassung”). Für die Objektklassen `vipUser`, `vipGroup` und `vipRole` muss der Objektklassentyp “Zusätzlich” gewählt werden.

Fügen Sie nach dem Einrichten der Objektklassen die Objektklasse `vipUser` der in Active Directory vordefinierten Objektklasse `user` als Erweiterungsklasse hinzu. Die Objektklassen `vipGroup` und `vipRole` müssen der in Active Directory vordefinierten Objektklasse `group` als Erweiterungsklasse hinzugefügt werden. Wenn Sie die Option *Sammelgruppen/-rollen* nutzen, müssen Sie die Objektklassen `vipGroup` und `vipRole` zusätzlich den Sammelobjektklassen (z.B. `organizationalUnit`) als Erweiterungsklassen hinzufügen.

Durch die Festlegung der WCM-Objektklassen auf den jeweiligen Objektklassentyp können vorhandene Einträge der Objektklasse `user` bzw. `group` über dem Admin-Client um die WCM-spezifischen Attribute erweitert werden (siehe Kapitel “Benutzerverwaltung” im Livelink WCM Server-Administratorhandbuch).

Benutzer, Gruppen und Rollen können mithilfe des Admin-Clients im LDAP-Server neu angelegt werden. Voraussetzung dafür ist, dass Sie bei der Installation des WCM-Systems die in Active Directory für Benutzer, Gruppen und Rollen vordefinierten Objektklassen `user` und `group` angeben (siehe Abschnitt “WCM-spezifische LDAP-Parameter angeben” auf Seite 90). In den Einstellungen des LDAP-Pools muss außerdem unter *Namensgebendes Attribut für Benutzer* der Eintrag “cn” ausgewählt werden.

Attribute

Active Directory verwendet das Attribut `cn` als namensgebendes Attribut für den LDAP-Eintrag. Der Wert des namensgebenden Attributs muss eindeutig sein. Mehrwertige “relative distinguished names” (RDN) können von Livelink WCM Server nicht ausgewertet werden.

Die folgende Tabelle zeigt die WCM-Attribute, ihr Vorhandensein in Active Directory, den jeweiligen Datentyp und das entsprechende Mapping der WCM- auf die LDAP-Attribute.

Hinweise zum Anlegen der Objektklassen und Attribute

- Existieren einige der aufgeführten Attribute bereits im LDAP-Server, können sie den WCM-Klassen einfach zugeordnet werden, wenn sie die richtige Semantik und Syntax aufweisen.
- Existieren einige Attribute bereits im LDAP-Server, die zwar gültige Werte, aber andere Namen haben, ordnen Sie die benötigten WCM-Attribute den vorhandenen LDAP-Attributen zu. Dies wird als *Mapping* bezeichnet. Die Standard-Mapping-Paare sind in der folgenden Tabelle aufgeführt. Die Vorgehensweise beim Mapping ist im Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45 beschrieben.
- Existieren einige Attribute bereits im LDAP-Server, die zwar den gleichen Namen, aber ungültige Werte haben, müssen Sie zusätzliche benutzerdefinierte Attribute anlegen.
- In der Spalte “Single-Value” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut ein Single-Value ist. Ist dort ein Haken gesetzt, **muss** der Attributwert einwertig sein. Im LDAP-Verzeichnisdienst kann als Typ des Attributs trotzdem “Multi-Value” (mehrwertig) eingestellt sein – es muss jedoch sichergestellt sein, dass das Attribut nur über einen Wert verfügt. Ansonsten ist die korrekte Auswertung des Attributs durch Livelink WCM Server nicht gewährleistet.

- In der Spalte “Obligatorisch” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut einen Wert hat. Ist dort ein Haken gesetzt, **muss** das Attribut einen Wert haben.

Tabelle 24 – WCM-Attribute für die Klasse `vip` (Active Directory)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in Active Directory	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`vipAccess`	case ignore string			✓	✓
`vipWebsite`	case ignore string				
`vipFuncarea`	case ignore string				
`vipRights`	case ignore string				✓
`vipType`	case ignore string			✓	✓

Tabelle 25 – WCM-Attribute für die Klasse `vipUser` (Active Directory)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in Active Directory	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`cn`		✓		✓	✓
`uid`		✓	`uid` → `samaccountname`	✓	✓
`email`		✓	`email` → `mail` (Standard-Mapping)	✓	✓
`vipLanguage`	case ignore string			✓	✓
`vipUserpassword`		✓		✓	✓
	Hinweis: Bitte beachten Sie die Erläuterungen im Abschnitt “Erweiterte Konfiguration für Active Directory” auf Seite 250.				
`initPassword`	case ignore string			✓	✓
`trustedLogin`	case ignore string			✓	✓
`vipSubstitute`	DN				✓
`hclProfiles`	case exact string				
`vipDomain`	case ignore string				

Tabelle 26 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (Active Directory)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in Active Directory	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`cn`		✓		✓	✓
`member`		✓			
`email`		✓	`email` → `mail` (Standard-Mapping)		✓

Hinweis: Durch die Verwendung so genannter *inverser LDAP-Attribute* wie z.B. `memberof` können Sie das Abfragen von Benutzerdaten beschleunigen, siehe Abschnitt “LDAP-Abfragen beschleunigen” auf Seite 54.

Erweiterte Konfiguration für Active Directory

Bestimmte Funktionen erfordern für Active Directory spezielle Mapping-Einträge, die Sie vor der Installation in der Datei **defaults.xml** bzw. nach der Installation in der Datei **ldapmapping.xml** vornehmen (siehe Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45). Im Folgenden finden Sie eine Übersicht über diese Mapping-Einträge:

- Ändern des Passworts über Livelink WCM Server

```
<USER_PASSWORD>
   <vipattr>vipUserpassword</vipattr>
   <ldapattr>unicodePwd</ldapattr>
   <ldapread>false</ldapread>
   <ldapwrite>true</ldapwrite>
   <codec>de.gauss.vip.jndi.codec.ADSUnicodePwd</codec>
```

```
</USER_PASSWORD>
```

Hinweis: Damit die Passwörter über Livelink WCM Server geändert werden können, muss die Kommunikation zum LDAP-Server über gesicherte Verbindungen (SSL) erfolgen. Wenn keine SSL-Verbindung möglich ist, setzen Sie das Tag `<ldapwrite>` auf den Wert `false`.

- Anlegen von Gruppen und Rollen über Livelink WCM Server

```
<ADS_ACCOUNTNAME>
   <vipattr>sAMAccountName</vipattr>
   <ldapattr>sAMAccountName</ldapattr>
   <ldapread>false</ldapread>
   <ldapwrite>true</ldapwrite>
   <ldapdef>$cn</ldapdef>
</ADS_ACCOUNTNAME>
```

- Aktivieren von Benutzer-Konten

  Üblicherweise sind in Active Directory Benutzer-Konten, die über LDAP angelegt werden, deaktiviert. Damit die Konten sofort aktiviert sind, ist folgender Eintrag erforderlich:

```
<ADS_ACCOUNTCONTROL>
   <vipattr>userAccountControl</vipattr>
   <ldapattr>userAccountControl</ldapattr>
   <ldapread>false</ldapread>
   <ldapwrite>true</ldapwrite>
</ADS_ACCOUNTCONTROL>
```

A.2 Novell eDirectory (NDS)

Hinweise

- Die im Folgenden beschriebene Konfiguration basiert auf der Annahme, dass die Verwaltung der WCM-Benutzer auf Grundlage eines bestehenden NDS-Verzeichnisdienstes realisiert wird. Wenn Sie Novell eDirectory ausschließlich zur Verwaltung der WCM-Benutzer und nicht zur Verwaltung der Benutzer des Firmennetzwerks verwenden, sind unter Umständen andere Einstellungen notwendig. Wir empfehlen die Zusammenarbeit mit der Professional Services Group der Gauss Interprise AG.
- Wenn Sie kein SSL für den Zugriff von Livelink WCM Server auf den LDAP-Verzeichnisdienst nutzen, erfolgt die Übertragung der Passwörter im Klartext. Dies muss in der Konfiguration von Novell eDirectory freigeschaltet werden. Sie finden die entsprechende Option in der NDS-Administrationskonsole (ConsoleOne), indem Sie den Wurzelkontext markieren und dann im rechten Fensterbereich Folgendes auswählen: *LDAP Group* → *Properties* → Register *General*.
- Der Zugriff auf Novell eDirectory durch andere Systeme wie z.B. Livelink WCM Server muss in der Konfiguration von NDS aktiviert sein. Das entsprechende Vorgehen ist in der Dokumentation zu Novell eDirectory beschrieben.

Beim Verzeichnisdienst Novell eDirectory sind folgende Besonderheiten bei der Einrichtung von Objektklassen und Attributen zu beachten.

Objektklassen

Die Objektklasse `vip` muss als abstrakte Basisklasse aller WCM-spezifischen Objektklassen angelegt werden (NDS-Objektklassentyp = “Non-Effective”). Für die Objektklassen `vipUser`, `vipGroup` und `vipRole` muss der NDS-Objektklassentyp “Auxiliary” gewählt werden.

Durch die Festlegung der WCM-Objektklassen auf den jeweiligen NDS-Objektklassentyp können vorhandene NDS-Einträge über den Admin-Client um die WCM-spezifischen Attribute erweitert werden (siehe Kapitel “Benutzerverwaltung” im Livelink WCM Server-Administratorhandbuch).

> **Hinweis:** Benutzer, Gruppen und Rollen können **nicht** über den Admin-Client im LDAP-Server angelegt werden. Das Neuanlegen von Benutzern, Gruppen und Rollen muss über ConsoleOne erfolgen.

Installation

Bei der Installation des WCM-Systems muss zum Speichern des Principal-Typs das Attribut `objectclass` gewählt werden (siehe Abschnitt “Parameter des LDAP-Verzeichnisdienstes einstellen” auf Seite 88).

Attribute

NDS kann das Attribut `cn` oder `uid` (auch `uniqueID`) als namensgebendes Attribut für den LDAP-Eintrag verwenden. Aus Gründen der Eindeutigkeit empfiehlt es sich, dass Attribut `uid` zu verwenden.

Die folgende Tabelle zeigt die WCM-Attribute, ihr Vorhandensein in NDS, den jeweiligen Datentyp und das entsprechende Mapping der WCM- auf die LDAP-Attribute.

Hinweise zum Anlegen der Objektklassen und Attribute

- Existieren einige der aufgeführten Attribute bereits im LDAP-Server, können sie den WCM-Klassen einfach zugeordnet werden, wenn sie die richtige Semantik und Syntax aufweisen.
- Existieren einige Attribute bereits im LDAP-Server, die zwar gültige Werte, aber andere Namen haben, ordnen Sie die benötigten WCM-Attribute den vorhandenen LDAP-Attributen zu. Dies wird als *Mapping* bezeichnet. Die Standard-Mapping-Paare sind in der folgenden Tabelle aufgeführt. Die Vorgehensweise beim Mapping ist

im Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45 beschrieben.

- Existieren einige Attribute bereits im LDAP-Server, die zwar den gleichen Namen, aber ungültige Werte haben, müssen Sie zusätzliche benutzerdefinierte Attribute anlegen.
- In der Spalte “Single-Value” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut ein Single-Value ist. Ist dort ein Haken gesetzt, **muss** der Attributwert einwertig sein. Im LDAP-Verzeichnisdienst kann als Typ des Attributs trotzdem “Multi-Value” (mehrwertig) eingestellt sein – es muss jedoch sichergestellt sein, dass das Attribut nur über einen Wert verfügt. Ansonsten ist die korrekte Auswertung des Attributs durch Livelink WCM Server nicht gewährleistet.
- In der Spalte “Obligatorisch” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut einen Wert hat. Ist dort ein Haken gesetzt, **muss** das Attribut einen Wert haben.

Tabelle 27 – WCM-Attribute für die Klasse `vip` (NDS)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in NDS	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`vipAccess`	boolean			✓	✓
`vipRights`	case ignore string				✓
`vipWebsite`	case ignore string				

WCM-Attribut	Datentyp (Syntax)	Vorhanden in NDS	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
vipFuncarea	case ignore string				
vipType[a]	case ignore string				✓

(a) Wenn Sie das Attribut vipType nicht verwenden bzw. definieren, muss der Schreibzugriff für dieses Attribut ausgeschaltet werden. Dies erfolgt mithilfe entsprechender Mapping-Einträge in der Datei **defaults.xml** (<ldapwrite>false</ldapwrite>), siehe Abschnitt “Lesbarkeit und Schreibbarkeit der LDAP-Attribute steuern” auf Seite 51.

Tabelle 28 – WCM-Attribute für die Klasse vipUser (NDS)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in NDS	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
cn		✓		✓	✓
uid		✓	uid → uniqueId	✓	✓
email	case ignore string	✓	email → mail[a] (Standard-Mapping)	✓	✓
vipLanguage	case ignore string			✓	✓

WCM-Attribut	Datentyp (Syntax)	Vorhanden in NDS	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
vipUserpassword[b]		✓	vipUserpassword → userPassword (Standard-Mapping)	✓	✓
initPassword	boolean			✓	✓
trustedLogin	boolean			✓	✓
vipSubstitute	DN (mit Attribut-synchronisa-tion)				✓
hclProfiles	case exact string				
vipDomain	case ignore string				

(a) In der Oberfläche von ConsoleOne wird für dieses Attribut der Name “Internet EMail Address” verwendet. Novell eDirectory mappt diesen Namen intern auf den LDAP-Namen “mail”. Aus diesem Grund muss in der Mapping-Datei **defaults.xml** das Mapping so erfolgen wie in der Tabelle angegeben, d.h., es muss der LDAP-Name des Attributs verwendet werden.

(b) Bei Novell eDirectory muss der Lesezugriff für das Attribut `vipUserpassword` ausgeschaltet werden. Dies erfolgt mithilfe entsprechender Mapping-Einträge in der Datei **defaults.xml** (`<ldapread>false</ldapread>` und `<ldapwrite>true</ldapwrite>`), siehe Abschnitt “Lesbarkeit und Schreibbarkeit der LDAP-Attribute steuern” auf Seite 51.

Tabelle 29 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (NDS)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in NDS	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`cn`		✓		✓	✓
`member`		✓	`member` → `uniqueMember`[a]		
`email`	case ignore string		`email` → `mail` (Standard-Mapping)		✓

(a) In der Oberfläche von ConsoleOne wird für dieses Attribut der Name “Member” verwendet. Novell eDirectory mappt diesen Namen intern auf den LDAP-Namen “uniqueMember”. Aus diesem Grunde muss in der Mapping-Datei **defaults.xml** das Mapping so erfolgen wie in der Tabelle angegeben, d.h., es muss der LDAP-Name des Attributs verwendet werden.

A.3 Sun ONE Directory Server

Beim Verzeichnisdienst Sun ONE sind folgende Besonderheiten zu beachten.

Objektklassen

Die Objektklasse `vip` sollte als Objektklasse aller WCM-spezifischen Objektklassen (`vipUser`, `vipGroup` und `vipRole`) angelegt werden. Objektklassen bei Sun ONE erlauben prinzipiell die Erweiterung bestehender Profile um zusätzliche Attribute und das Neuanlegen von Profilen. Benutzer, Gruppen und Rollen können somit mithilfe des Admin-Clients im LDAP-Server neu angelegt werden. Existierende LDAP-Einträge können

außerdem um die WCM-spezifischen Attribute erweitert werden (siehe Kapitel “Benutzerverwaltung” im Livelink WCM Server-Administratorhandbuch).

Attribute

Die folgende Tabelle zeigt die WCM-Attribute, ihr Vorhandensein in Sun ONE, den jeweiligen Datentyp und das entsprechende Mapping der WCM- auf die LDAP-Attribute.

Hinweise zum Anlegen der Objektklassen und Attribute

- Existieren einige der aufgeführten Attribute bereits im LDAP-Server, können sie den WCM-Klassen einfach zugeordnet werden, wenn sie die richtige Semantik und Syntax aufweisen.
- Existieren einige Attribute bereits im LDAP-Server, die zwar gültige Werte, aber andere Namen haben, ordnen Sie die benötigten WCM-Attribute den vorhandenen LDAP-Attributen zu. Dies wird als *Mapping* bezeichnet. Die Standard-Mapping-Paare sind in der folgenden Tabelle aufgeführt. Die Vorgehensweise beim Mapping ist im Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45 beschrieben.
- Existieren einige Attribute bereits im LDAP-Server, die zwar den gleichen Namen, aber ungültige Werte haben, müssen Sie zusätzliche benutzerdefinierte Attribute anlegen.
- In der Spalte “Single-Value” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut ein Single-Value ist. Ist dort ein Haken gesetzt, **muss** der Attributwert einwertig sein. Im LDAP-Verzeichnisdienst kann als Typ des Attributs trotzdem “Multi-Value” (mehrwertig) eingestellt sein – es muss jedoch sichergestellt sein, dass das Attribut nur über einen Wert verfügt. Ansonsten ist die korrekte Auswertung des Attributs durch Livelink WCM Server nicht gewährleistet.

- In der Spalte “Obligatorisch” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut einen Wert hat. Ist dort ein Haken gesetzt, **muss** das Attribut einen Wert haben.

Tabelle 30 – WCM-Attribute für die Klasse `vip` (Sun ONE)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in Sun ONE	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`vipAccess`	boolean			✓	✓
`vipRights`	directory string				✓
`vipWebsite`	directory string				
`vipFuncarea`	directory string				
`vipType`[a]	directory string				✓

(a) Wenn Sie das Attribut `vipType` nicht verwenden bzw. definieren, muss der Schreibzugriff für dieses Attribut ausgeschaltet werden. Dies erfolgt mithilfe entsprechender Mapping-Einträge in der Datei **defaults.xml** (`<ldapwrite>false</ldapwrite>`), siehe Abschnitt “Lesbarkeit und Schreibbarkeit der LDAP-Attribute steuern” auf Seite 51.

Tabelle 31 – WCM-Attribute für die Klasse `vipUser` (Sun ONE)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in Sun ONE	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`cn`		✓		✓	✓
`uid`		✓		✓	✓
`email`		✓	`email` → `mail` (Standard-Mapping)	✓	✓
`vipLanguage`	directory string			✓	✓
`vipUserpassword`		✓	`vipUserpassword` → `userPassword` (Standard-Mapping)	✓	✓
`initPassword`	boolean			✓	✓
`trustedLogin`	boolean			✓	✓
`vipSubstitute`	DN				✓
`hclProfiles`	directory string				
`vipDomain`	directory string				

Tabelle 32 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (Sun ONE)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in Sun ONE	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`cn`		✓		✓	✓
`member`		✓			
`email`		✓	`email` → `mail` (Standard-Mapping)		✓

A.4 OpenLDAP

Beim Verzeichnisdienst OpenLDAP sind folgende Besonderheiten zu beachten.

Hinweis

Die folgenden “includes” sollten in der Datei **slapd.conf** definiert werden:

```
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/misc.schema
include /usr/local/etc/openldap/schema/openldap.schema
```

Objektklassen

Die Objektklasse `vip` sollte als Objektklasse aller WCM-spezifischen Objektklassen (`vipUser`, `vipGroup` und `vipRole`) angelegt werden. Objektklassen bei OpenLDAP erlauben prinzipiell die Erweiterung bestehender Profile um zusätzliche Attribute und das Neuanlegen von Profilen. Benutzer, Gruppen und Rollen können somit mithilfe des Admin-Clients im LDAP-Server neu angelegt werden. Existierende LDAP-Einträge können außerdem um die WCM-spezifischen Attribute erweitert werden (siehe Kapitel “Benutzerverwaltung” im Livelink WCM Server-Administratorhandbuch).

Attribute

Die folgende Tabelle zeigt die WCM-Attribute, ihr Vorhandensein in OpenLDAP, den jeweiligen Datentyp und das entsprechende Mapping der WCM- auf die LDAP-Attribute.

Hinweise zum Anlegen der Objektklassen und Attribute

- Existieren einige der aufgeführten Attribute bereits im LDAP-Server, können sie den WCM-Klassen einfach zugeordnet werden, wenn sie die richtige Semantik und Syntax aufweisen.
- Existieren einige Attribute bereits im LDAP-Server, die zwar gültige Werte, aber andere Namen haben, ordnen Sie die benötigten WCM-Attribute den vorhandenen LDAP-Attributen zu. Dies wird als *Mapping* bezeichnet. Die Standard-Mapping-Paare sind in der folgenden Tabelle aufgeführt. Die Vorgehensweise beim Mapping ist im Abschnitt “WCM-Attribute auf LDAP-Attribute mappen” auf Seite 45 beschrieben.
- Existieren einige Attribute bereits im LDAP-Server, die zwar den gleichen Namen, aber ungültige Werte haben, müssen Sie zusätzliche benutzerdefinierte Attribute anlegen.

- In der Spalte “Single-Value” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut ein Single-Value ist. Ist dort ein Haken gesetzt, **muss** der Attributwert einwertig sein. Im LDAP-Verzeichnisdienst kann als Typ des Attributs trotzdem “Multi-Value” (mehrwertig) eingestellt sein – es muss jedoch sichergestellt sein, dass das Attribut nur über einen Wert verfügt. Ansonsten ist die korrekte Auswertung des Attributs durch Livelink WCM Server nicht gewährleistet.
- In der Spalte “Obligatorisch” ist jeweils gekennzeichnet, ob das WCM-System erwartet, dass das Attribut einen Wert hat. Ist dort ein Haken gesetzt, **muss** das Attribut einen Wert haben.

Tabelle 33 – WCM-Attribute für die Klasse `vip` (OpenLDAP)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in OpenLDAP	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`vipAccess`	directory string			✓	✓
`vipRights`	directory string				✓
`vipWebsite`	directory string				
`vipFuncarea`	directory string				
`vipType`[a]	directory string				✓

(a) Wenn Sie das Attribut `vipType` nicht verwenden bzw. definieren, muss der Schreibzugriff für dieses Attribut ausgeschaltet werden. Dies erfolgt mithilfe entsprechender Mapping-Einträge in der Datei **defaults.xml** (`<ldapwrite>false</ldapwrite>`), siehe Abschnitt “Lesbarkeit und Schreibbarkeit der LDAP-Attribute steuern” auf Seite 51.

Tabelle 34 – WCM-Attribute für die Klasse `vipUser` (OpenLDAP)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in OpenLDAP	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`cn`		✓		✓	✓
`uid`		✓		✓	✓
`email`		✓	`email` → `mail` (Standard-Mapping)	✓	✓
`vipLanguage`	directory string			✓	✓
`vipUserpassword`		✓	`vipUserpassword` → `userPassword` (Standard-Mapping)	✓	✓
`initPassword`	directory string			✓	✓
`trustedLogin`	directory string			✓	✓
`vipSubstitute`	DN				✓
`hclProfiles`	directory string				
`vipDomain`	directory string				

Tabelle 35 – WCM-Attribute für die Klassen `vipGroup` und `vipRole` (OpenLDAP)

WCM-Attribut	Datentyp (Syntax)	Vorhanden in OpenLDAP	Mapping WCM-Attribut → LDAP-Attribut	Obligatorisch	Single-Value
`cn`		✓		✓	✓
`member`		✓			
`email`		✓	`email` → `mail` (Standard-Mapping)		✓

Glossar

ACL – Access Control List, siehe *Zugriffssteuerungsliste*

Adresse – siehe *URL*

API – Application Programming Interface. Livelink WCM Server bietet verschiedene APIs, um auf die Funktionalitäten der WCM-Server zuzugreifen: das WCM Java API, das Remote-API, das Portal Manager API und WCM WebServices.

Applet – Java-Programm, das in eine Website eingebettet ist. Ein Applet wird vom Server geladen und auf dem Client ausgeführt.

Application-Server – Auch Enterprise-Application-Server. Eine Infrastruktur, die als Middleware und/oder Entwicklungs- und Laufzeitumgebung für Web- und Wireless-Anwendungen fungiert. Ein Application-Server interagiert mit dem API (Application Programming Interface). Dadurch bietet er mehr Flexibilität und ermöglicht die Ausführung komplexerer Aufgaben an einem entfernten Rechner oder über das Internet.

Auf diese Weise wird die Kommunikation zwischen Server und Benutzer einer Webseite verbessert, sodass der Benutzer z.B. eine Datenbank abfragen kann oder Programme ausführen kann, die auf dem Server installiert sind. Application-Server bieten häufig zusätzlich Sicherheitsmerkmale, Lastenverteilung (load balancing) und Ausfallmechanismen (failover mechanisms) sowie Skalierungs- und Integrationsfunktionen.

ASP – Active Server Pages. HTML-Dateien mit besonders gekennzeichneten eingebetteten JavaScript- bzw. Visual Basic Script-Programmen, die im Webserver ausgeführt werden. Das Ergebnis wird dann im normalen HTML-Format an den Client gesendet.

Attribute – Spezielle Metadaten, die für jeden Objekttyp unterschiedlich definiert werden können. Attribute werden in Attributmengen zusammengefasst.

Attributmenge – Menge von Attributen. Attributmengen können mit Objekttypen verbunden werden. Auf diese Weise werden alle WCM-Objekte, die auf Grundlage dieses Objekttyps erstellt werden, mit den Attributen der zugeordneten Attributmenge ausgestattet. Die Bearbeitung von Attributmengen erfolgt im Admin-Client oder im Content-Client.

Cache – Zwischenspeicher zwischen langsamen und schnellen Einheiten, in dem häufig benötigte Daten abgelegt werden. Ein Cache wird zur Reduzierung von Zugriffszeiten benutzt.

CGI – Common Gateway Interface. Eine Schnittstelle der Webserver, um Skripte oder Programme auszuführen, die Benutzerantworten auf HTML-Formulare erzeugen. Üblicherweise befinden sich CGI-Programme in einem speziellen Verzeichnis des HTTP-Servers. Spezielle URLs rufen ein solches CGI-Programm auf, das eine HTML-Antwortseite auf die Anfrage generiert und an den Client sendet.

Context-ID – Objekt, das einem Benutzer nach erfolgreicher Anmeldung am WCM-System zugeteilt wird. Eine Context-ID ist immer systemweit eindeutig, sie identifiziert deshalb genau einen Benutzer. Wird eine Context-ID eine gewisse Zeit nicht gebraucht, so verfällt sie.

Datenbank – Strukturierter, inhaltlich zusammengehöriger Datenbestand, der von einem Datenbank-Managementsystem verwaltet wird

DBMS – Datenbank-Managementsystem. Ein DBMS ermöglicht den kontrollierten Zugriff auf Datenbanken und deren Verwaltung.

Deployment – Deployment bezeichnet die Verteilung von Daten. Das Deployment von Livelink WCM Server übernimmt zwei Hauptaufgaben: erstens die Generierung von Seiten aus den in der Datenbank gespeicherten WCM-Objekten und die Verteilung der generierten Dateien in die dafür vorgesehenen Verzeichnisse; zweitens die Benachrichtigung der WCM-Server bei Änderungen im WCM-System.

Deploymentsystem – Die Deploymentsysteme erzeugen aus den WCM-Objekten Seiten und verteilen die generierten Dateien in die dafür vorgesehenen Verzeichnisse. Von dort aus werden die Dateien über den Einsatz eines HTTP-Servers für die Benutzer sichtbar. Deploymentsysteme können unterschiedliche Typen und Kategorien haben.

Deploymentsystem-Kategorie – Je nach Art der Verarbeitung von Deploymentaufträgen werden Deploymentsysteme verschiedenen Kategorien zugeordnet: *Standard-Deploymentsysteme* erzeugen bei jeder Änderung an einem WCM-Objekt automatisch eine neue Seite. Die generierten Seiten werden im Dateisystem abgelegt. *Dynamische Deploymentsysteme* generieren die Seiten auf Grundlage benutzerdefinierter Einstellungen und nur dann, wenn die Seite über den HTTP-Server angefordert wird. Die generierten Dateien werden in einer flachen Dateistruktur abgelegt. Mit *Suchmaschinen-Deploymentsystemen* können Sie die Daten Ihrer Website für den Einsatz einer Suchmaschine aufbereiten. *WebDAV-Deploymentsysteme* bilden die Voraussetzung für den Einsatz von WebDAV-Clients. *InSite Editing-Deploymentsysteme* schaffen die Voraussetzung dafür, dass Inhalte direkt innerhalb der Website – ohne Content-Client – bearbeitet und hinzugefügt werden können.

Deploymentsystem-Typen – Bei Deploymentsystemen wird entsprechend dem Staging-Konzept von Livelink WCM Server zwischen den Typen “Edit”, “QS” und “Produktion” unterschieden. Je nach Typ werden unterschiedliche Sichten auf die Daten der Website erzeugt.

Edit-Sicht – In der Edit-Sicht von Livelink WCM Server werden die Objekte einer Website angelegt und redaktionell bearbeitet. Hier ist der jeweils aktuelle Bearbeitungsstand zu sehen.

Extranet – Auf Internet-Technologien basierte Informationsplattform für die Unternehmenskommunikation mit autorisierten externen Benutzern, z. B. Partnern oder Kunden

Firewall – Hard- oder Software, die den Datenfluss zwischen einem öffentlichen und einem privaten Netz kontrolliert und gegen unberechtigte Zugriffe schützt. Livelink WCM Server unterstützt Firewall-geschützte Architekturen.

Formular – Möglichkeit, vom Benutzer auszufüllende Dialogelemente in Web-Seiten einzubauen. Der Inhalt eines solchen Formulars kann zur Weiterverarbeitung an den Server gesendet werden.

Frame-Objekt – Objekttyp für ein Frameset

Frame-Thema – Frame-Objekt, das gleichzeitig als Thema (zur inhaltlichen Organisation) verwendet wird. Siehe auch *Thema*.

Gruppe – Zusammenstellung von Benutzern, für die bestimmte Zugriffsrechte definiert werden können. Benutzergruppen sind in der Regel an Organisationseinheiten wie Abteilungen oder Projekte geknüpft.

Gruppenrolle – Kombination aus einer Gruppe und einer Rolle. Bei der Gruppenrolle handelt es sich nicht um eine Organisationseinheit, die im Admin-Client definiert wird, sondern um eine Einstellungsmöglichkeit für die Objekt-Zugriffsrechte im Content-Client.

HTTP – Hypertext Transfer Protocol. Ein Kommunikationsprotokoll zum Transfer von HTML-Seiten.

HTTP-Server – Ein HTTP-Server bietet einem HTTP-Client (Browser) HTTP-Dienste an einem standardisierten TCP/IP-Port an.

HTTP-Tunneling – Beim HTTP-Tunneling werden die Daten innerhalb eines WCM-Systems verpackt als HTTP-Datenstrom übertragen. Dabei werden die Daten zuerst entsprechend dem Protokoll VIPP kodiert und anschließend zusätzlich in HTTP verpackt.

In Firewall-Szenarien ist HTTP-Tunneling ein gängiges Übertragungsverfahren. Firewall-Systeme interpretieren den Datenstrom und schalten u.a. nur bestimmte Protokolle frei. Wenn das Protokoll VIPP nicht freigeschaltet ist, können die Daten mithilfe von HTTP-Tunneling übertragen werden.

Java – Von Sun Microsystems entwickelte objektorientierte Programmiersprache, die vor allem im Bereich der Internet-Technologien genutzt wird. Sicherheitsaspekte und Plattformunabhängigkeit sind die Grundphilosophien von Java.

Java 2 SDK – Java 2 Software Development Kit. Das SDK enthält alle Komponenten, die für das Erstellen und Verwenden von Programmen und Applets in Java benötigt werden, d.h. den Java-Compiler, das Java Runtime Environment und diverse Hilfsprogramme.

JavaScript – Skriptsprache, um in HTML-Seiten ein ausführbares Script zu integrieren. Mittels JavaScript können Formulare mit Plausibilitätsprüfungen oder Berechnungsfunktionen versehen werden.

JDBC – Java Database Connectivity. Ein Mechanismus zur Kommunikation mit bestehenden Datenbanken. Dabei bilden Treiber die Schnittstelle zwischen dem Java-Programm und der Datenbank.

JRE – Java Runtime Environment. Das JRE enthält alle Komponenten, die für die Ausführung von Java-Programmen benötigt werden, d.h. die Java Virtual Machine und die Java-Klassenbibliothek.

JSP – JavaServer-Pages. HTML-Dateien mit besonders gekennzeichneten eingebetteten Java-Programmen, die mithilfe einer JSP-Engine einmalig in Servlets umgewandelt und anschließend im Webserver ausgeführt werden. Das Ergebnis wird dann im normalen HTML-Format (ohne Java) an den Client gesendet.

JVM – Java Virtual Machine. Die JVM ermöglicht die Ausführung der plattformunabhängigen Java-Programme auf einem bestimmten Rechner. Sie ist Teil des JDK bzw. der JRE.

LDAP – Lightweight Directory Access Protocol. Das LDAP basiert auf dem X.500-Standard und wird von den meisten großen Softwareherstellern unterstützt. LDAP-Verzeichnisdienste dienen zum Verwalten von Benutzerinformationen.

Master-Server – Nur Master-Server haben lesenden und schreibenden Zugriff auf die Daten eines WCM-Systems. Der Master-Content-Server verwaltet die Website-Daten, der Master-Administrationsserver die Konfigurations- und Systemdaten des WCM-Systems. Siehe auch *Serverkategorie*.

Metadaten – Jedem WCM-Objekt sind eine Reihe von Objektinformationen (wie z. B. Ablaufdatum, Sprache) zugeordnet. Diese werden als Metadaten bezeichnet.

Objektkategorie – Zuordnung eines WCM-Objekts zu einer bestimmten Kategorie. Aufgrund dieser Zuordnung hat das WCM-Objekt eine Reihe von zusätzlichen Spezialattributen (Metadaten).

Objekttyp – Bezeichnet die spezifische Art des jeweiligen Objekts, z. B. “HTML-Seite”, “HTML-Vorlage”, “Thema”. Aus dem Objekttyp ergeben sich verschiedene Eigenschaften des WCM-Objekts. Der Objekttyp wird beim Anlegen des Objekts festgelegt und kann für einige Objekttypen nachträglich geändert werden. Objekttypen können über den Admin-Client oder den Content-Client bearbeitet werden.

Pool – Die verschiedenen Verbindungen innerhalb eines WCM-Systems werden in Pools verwaltet. Dazu zählen z. B. Verbindungen für die Kommunikation mit einem LDAP-Verzeichnisdienst oder zwischen den WCM-Servern. Wird eine Verbindung benötigt, wird sie aus dem jeweiligen Pool zur Verfügung gestellt. Nach Abschluss der Datenübertragung wird die Verbindung an den Pool zurückgegeben. Pools fassen immer Verbindungen desselben Typs zusammen, also z. B. Verbindungen zu Datenbanken (JDBC-Pools) oder Verbindungen zwischen WCM-Servern (WCM-Pools).

Portal – Als Portal wird eine Website bezeichnet, die dem Benutzer als zentraler Einstieg – als Tor – in bestimmte Internetangebote dient. Ein Portal bietet oftmals themenbezogene, personalisierte Angebote und Informationen.

Produktionssicht – Die Produktionssicht von Livelink WCM Server stellt die freigegebenen Seiten einer Website bereit. Mithilfe eines Webservers kann auf die Seiten über das Internet, Intranet oder Extranet zugegriffen werden.

Proxy-Server – Ein Proxy-Server dient dazu, Anforderungen von einer Client-Anwendung, etwa einem Browser, an einen anderen (oder mehrere andere) Server abzufangen. Wenn der Proxy-Server die Anforderung erfüllen kann, sendet er die angeforderten Daten an die Client-Anwendung zurück. Andernfalls leitet er die Anforderung an den spezifizierten Server weiter.

Im Kontext von Livelink WCM Server haben WCM-Server der Kategorie “Proxy” keinen schreibenden, sondern nur lesenden Zugriff auf die WCM-Objekte bzw. die Konfiguration. Die Änderung von WCM-Objekten erfolgt ausschließlich über den Master-Content-Server, Änderungen an der Konfiguration des WCM-Systems sind nur über den Master-Administrationsserver möglich. Siehe auch *Serverkategorie*.

QS-Sicht – Die QS-Sicht von Livelink WCM Server dient der Qualitätssicherung der Objekte und damit der Website-Inhalte. Diese Sicht stellt also die Kontrollinstanz zwischen der Bearbeitung in der Edit-Sicht und der Veröffentlichung in der Produktionssicht dar.

RDBMS – Relationales Datenbank-Managementsystem. Ein DBMS, in dem Relationen zwischen den Datensätzen von einzelnen Datenbanken genutzt werden können. Im Unterschied dazu existieren auch objektorientierte und objektrelationale DBMS.

Relator – Durch die Integration von Web Content Management und Livelink ist es möglich, Livelink-Objekte in einer vom WCM-System verwalteten Website als WCM-Objekte anzulegen. Diese WCM-Objekte werden Relatoren genannt und beziehen sich immer auf eine bestimmte Version eines Livelink-Objekts. Für das Einbinden eines einzelnen Livelink-Objekts gibt es den WCM-Objekttyp “Livelink-Relator”; um einen

Ordner aus Livelink einzubinden, gibt es den WCM-Objekttyp “Livelink-Ordner-Relator”.

Rolle – Zusammenstellung von Benutzern, ähnlich wie eine Benutzergruppe, für die bestimmte Zugriffsrechte definiert werden können. Die Benutzerrolle wird meistens aufgabenbezogen definiert, während Benutzergruppen in der Regel an Organisationseinheiten wie Abteilungen oder Projekte geknüpft sind.

Serverkategorie – In einem WCM-System wird zwischen Master- und Proxy-Servern unterschieden. Master-Server haben schreibenden Zugriff auf die Daten des WCM-Systems, Proxy-Server dagegen nur lesenden. Der Master-Content-Server verwaltet die Website-Daten, der Master-Administrationsserver die Konfigurations- und Systemdaten. Darüber hinaus können beliebig viele Proxy-Server eingesetzt werden.

Servertyp – Entsprechend den Aufgaben der Server gibt es zwei Servertypen: Content-Server zur Verwaltung von Website-Daten und Administrationsserver zur Verwaltung der Benutzer-, Konfigurations- und Systemdaten des WCM-Systems. Jeder Content-Server ist grundsätzlich dazu in der Lage, alle Sichten auf die Daten der verwalteten Website(s) zur Verfügung zu stellen – Edit, QS und Produktion. Die verfügbaren Sichten können dadurch eingeschränkt werden, dass der Content-Server nur die Daten von bestimmten Sichten erhält.

Servlet – Vom Webserver ausgeführtes Java-Programm zur Generierung der von einem Client mittels HTTP-Request angeforderten Daten

SMTP – Simple Mail Transfer Protocol. Ein Protokoll für den Transfer von E-Mail-Nachrichten, z.B. zwischen verschiedenen Servern

SSL – Secure Socket Layer. Protokollschicht für die Kommunikation zwischen den Komponenten eines WCM-Systems, die für eine abhör- und verfälschungssichere Datenübertragung sorgt. SSL kann sowohl für das Protokoll VIPP als auch für HTTP-Tunneling verwendet werden.

Statifizierung – Beim Statifizieren werden die dynamischen Bestandteile z. B. einer JSP-Seite in statische umgewandelt. Das Ergebnis ist reines HTML ohne Java-Code.

Suchserver – Das Index- und Query-System werden innerhalb von Livelink WCM Server unter dem Begriff “Suchserver” zusammengefasst. Ein Suchserver ist immer genau einem WCM-Server zugeordnet. Einem WCM-Server können auch mehrere Suchserver zugeordnet sein.

TCP/IP – Transmission Control Protocol/Internet Protocol. Basisprotokoll für die Übertragung von Daten im Internet

Thema – Kombination aus einer HTML-Seite zur direkten Darstellung von Informationen und einem Verzeichnis für die Aufnahme von untergeordneten Objekten. Die Themen werden im Objektbaum als Knotenpunkt dargestellt und dienen damit auch zur Strukturierung der Website.

Typ – siehe *Objekttyp*

URL – Uniform Resource Locator. Eine eindeutige Adresse im World Wide Web.

VIPP – VIP Protocol. Proprietäres Protokoll zum Austausch von Daten zwischen den Komponenten eines WCM-Systems. Für die Kommunikation in WANs oder über das Internet kann VIPP in HTTP getunnelt werden.

WCM-Server – In einem WCM-System gibt es mehrere parallel arbeitende WCM-Server (Serverprozesse). Die genauen Aufgaben eines Servers hängen von Servertyp und Serverkategorie ab.

WCM-Tag – Spezialbaustein zur Einbindung von WCM-spezifischen Daten in einer HTML-Seite. Die WCM-Tags werden insbesondere bei der Erstellung von Vorlagen verwendet.

WebDAV – Das Protokoll WebDAV (Web-based Distributed Authoring and Versioning) unterstützt ein Internet- und gruppenbasiertes Arbeiten auf Grundlage von Standard-Internet-Technologien. So wird es Anwendern

ermöglicht, ohne einen speziellen Client WCM-Objekte mithilfe von WebDAV-fähigen Tools zu erstellen, gemeinsam daran zu arbeiten und diese zu verwalten.

Web-Repository – Als Web-Repository wird der Bereich bezeichnet, in dem sämtliche Objekte einer Website durch das WCM-System abgelegt und verwaltet werden.

Webserver – Programm zur Bearbeitung der Anforderungen eines Browsers. Ein Webserver entspricht einem HTTP-Server, der weitere Webdienste anbietet wie z.B. die einer JSP-Engine.

Webtechnologie – Client/Server-Technologie, die auf TCP/IP basiert. Der Vorteil liegt in dem offenen Standard, wodurch sich heterogene Systeme verwirklichen lassen.

Zugriffssteuerungsliste – Für jedes WCM-Objekt können Benutzer, Gruppen, Rollen und Gruppenrollen festgelegt werden, die Zugriff auf dieses Objekt haben sollen. Die einzelnen Zugriffsrechte werden für jeden Zugriffsberechtigten separat festgelegt. Wird auch als ACL (Access Control List) bezeichnet.

Index

A

Active Directory
  Konfiguration 246
Admin-Client
  Installation 122
Administrator
  bei der Installation angeben 93
  für Livelink WCM Server in LDAP einrichten 58
Admin-Server
  Installation 79
Alias für Content-Client 190
Apache 2
  Konfiguration 180
Application-Server
  Mapping 103
  Standardanwendung 103
Arbeitsspeicher
  für WCM-Server 166
Archivelog-Modus (Oracle) 23
Attribute (LDAP) für Livelink WCM Server 40

B

Base-Authentifizierung 192
  Konfiguration in IIS 193
BEA WebLogic 8.1
  Konfiguration 183
Benutzerverwaltung
  Art der Speicherung angeben 81
Beschleunigung von LDAP-Abfragen 54
Bindeprofil für LDAP-Verzeichnisdienst 57
Blockgröße (Oracle) 23

C

character-encoding (Secure Access-Parameter) 212
Content Miner
  deinstallieren 130
  installieren 105
  Ports festlegen 106
Content-Client
  Alias 190
  Encoding einstellen 99
  HTTPS-Verbindung 182, 184, 192
  in Webanwendung einbinden 102
  Precompile-Skript 202
Content-Server in Application-Server starten 170
Cursor (Oracle) 25

D

Datenbank
  allgemein 21
  anlegen in MS SQL Server 31
  Parameter bei der Installation 82
  Typ bei Installation angeben 83
Datenbankbenutzer
  anlegen in MS SQL Server 31
  anlegen in Oracle 27
Datenbankinstanzen (Oracle) 23
Datenbank-Zeichensatz (Oracle) 23
Datenquelle 85
Default application für Application-Server 103
defaults.xml für Installation/ Deinstallation 135
Deinstallation 130
  Datenbanktabellen löschen 134
  über grafische Oberfläche 132

über Konsole 135
Dienst
entfernen 133
für Admin-Server 81
für WCM-Server 100
Dienst in Windows
entfernen 133
für Admin-Server 81
für WCM-Server 100
directory-servlet (Secure Access-Parameter) 223

E

Eigentümer 85
Encoding
für Content-Client 99
für Secure Access 212
in Oracle einstellen 23
Explizite Zuordnung (LDAP) 38

F

Fallback-LDAP-Server 59
Filter-Mapping
für Webanwendung 104
filter-name (Secure Access-Parameter) 211
Firewall-Szenario
Installation 114

G

Gauss
LDAP-OIDs 43

H

Herunterfahren der Server 169
Hochfahren der Server 163
HTTP-Port 80, 98
httpport (Secure Access-Parameter) 214
HTTPS
für Verbindung zum Content-Client 182, 184, 192
für Verbindung zum LDAP-Server 64
HTTP-Server
Konfiguration für Secure Access 203, 206

I

Implizite Zuordnung (LDAP) 38
Index-System
separat starten (UNIX) 173
Installation
Admin-Client 122
Admin-Server 79
benutzerdefiniert 114
Content Miner 105
LDAP-Objektklassen für Livelink WCM Server 90
Livelink WCM Server (grafische Oberfläche) 71
Livelink WCM Server (Konsole) 135
Livelink-Suchserver 110
Lizenz erneuern 124
Lucene 108
Master-System hinter Firewall 115
minimal 72
Optionen für Lizenzdatei 77
Parameter des LDAP-Servers 88
Parameter des Livelink-Systems 86
Protokoll 174
Proxy-Content-Server hinter Firewall 116
Proxy-System vor Firewall 116
RDBMS-Parameter 82
Server einrichten 97
Server hinzufügen 118
starten über grafische Oberfläche 73
starten über Konsole 160

Steuerung 135
über Konsole 135
Verzeichnis 75
Verzeichnisstruktur danach 126
Voraussetzungen 14
Vorgehen 11
WCM-Administrator einrichten 93
Installationsprotokoll 174
Inverse LDAP-Attribute 54

J

Java 2 SDK 14
JDBC-Treiber
aktualisieren nach Patch 84
für Datenbank 83
JDK 14
JSP-Engine
Konfiguration für Secure Access 203, 207

K

Kommandozeilenmodus
Installation 135
Konfiguration
Apache 2 mit Tomcat 180
BEA WebLogic 8.1 183
für Secure Access 203
LDAP 35
Microsoft Active Directory 246
MS Internet Information Server mit Resin 185
MS SQL Server 31
Novell eDirectory 252
OpenLDAP 261
Oracle 22
RDBMS 21
Sun ONE Directory Server 257
Webserver 177
Konsole
Installation 135

L

Länderspezifischer Zeichensatz (Oracle) 23
LDAP
Attribute für beschleunige Abfragen mappen 54
Bindeprofil einrichten 57
ein LDAP-Server für mehrere WCM-Systeme 62
explizite Zuordnung von Benutzer 38
Fallback-LDAP-Server 59
implizite Zuordnung von Benutzern 38
Konfiguration 35
Lesbarkeit und Schreibbarkeit von Attributen 51
Mappen von WCM-Attributen auf LDAP-Attribute 45
mehrere LDAP-Server verwenden 59, 60
Microsoft Active Directory 246
Novell eDirectory 252
Objektklassen und Attribute für Livelink WCM Server 40
OIDs von Gauss 43
OpenLDAP 261
Parameter bei der Installation 88, 90
Sammelgruppen/-rollen 38
schnellere Abfragen 54
SSL-Verbindung zum LDAP-Server 64
Standardgruppen/-rollen 38
Sun ONE Directory Server 257
unterschiedliche Attribute für Namen 52
WCM-Administrator einrichten 58
ldapread (Tag für LDAP-Mapping) 51
ldapwrite (Tag für LDAP-Mapping) 51

Livelink
Parameter bei der Installation 86
Livelink WCM Server
Verzeichnisstruktur 127
Livelink-Suchserver
deinstallieren 130
installieren 110
Lizenzen
erneuern 124
Optionen bei Installation 77
log_checkpoint_interval (Oracle) 24
logdir (Secure Access-Parameter) 217
loglevel (Secure Access-Parameter) 216
logname (Secure Access-Parameter) 217
Lucene
deinstallieren 130
installieren 108

M

Mailserver
für Admin-Server 80
Mappen von WCM-Attributen auf LDAP-Attribute 45
Mapping für Webanwendungen 103
Master-System
Installation hinter Firewall 115
memberof (LDAP-Attribut) 54
Microsoft Active Directory
Konfiguration 246
Minimalinstallation 72
MS Internet Information Server
Authentifizierungsmethoden für Secure Access 192
Base-Authentifizierung konfigurieren 193
Einbinden von Resin 191
Konfiguration 186
NTLM-Authentifizierung konfigurieren 199
MS SQL Server 2000
Datenbank einrichten 31
Datenbankbenutzer anlegen 31
Konfiguration 31

N

NDS
Konfiguration 252
Neu
Server 118
Novell eDirectory
Konfiguration 252
NTLM-Authentifizierung 192
Konfiguration in IIS 199

O

Objektklassen für LDAP
einrichten 40
offene Cursor (Oracle) 25
open_cursors (Oracle) 24
OpenLDAP
Konfiguration 261
Oracle
Datenbankbenutzer anlegen 27
Datenbankinstanzen einrichten 23
JDBC-Treiber 83
Konfiguration 22
neuer JDBC-Treiber nach Patch 84
offene Cursor 25
Tabellenbereich einrichten 27
UTF-8 einstellen 23

P

parallel_max_servers 24
Parameter
defaults.xml für Installation/ Deinstallation 135

in Server-Startskripten 165
Patch für JDBC-Treiber 84
pathfrom (Secure Access-Parameter) 212
pathto (Secure Access-Parameter) 212
pattern (Secure Access-Parameter) 222
Performance
LDAP-Abfragen beschleunigen 54
Ports
für Content Miner bei Installation 106
für WCM-Server bei Installation 80, 98
Precompile-Skript für Content-Client 202
processes 24
profile (Secure Access-Parameter) 214
Protokolle
Installation 174
Secure Access 215
Proxy-Content-Server
Installation hinter Firewall 116
Proxy-System
Installation vor Firewall 116

Q

Query-System
separat starten (UNIX) 173

R

RDBMS
für Livelink WCM Server konfigurieren 21
neuer JDBC-Treiber nach Patch 84
Parameter bei der Installation 82
Tabellen nach Deinstallation löschen 134
Readme 127
realm (Secure Access-Parameter) 218
redirect-dir (Secure Access-Parameter) 219
redirect-url (Secure Access-Parameter) 219
Resin
Einbinden in MS Internet Information Server 191
Konfiguration 187
starten 191

S

Sammelgruppen/-rollen für LDAP 38
Schreibrechte für Verzeichnisse 126
secure (Secure Access-Parameter) 214
Secure Access
einbinden in HTTP-Server 206
einbinden in MS Internet Information Server 192
einstellen auf Unicode (UTF-8) 212
Konfiguration der JSP-Engine 207
Konfiguration von HTTP-Server und JSP-Engine 203
Konfiguration von Servlet bzw. Filter 207
Name des Webservers 214
Optionen für das Protokoll 215
Parameter von Servlet bzw. Filter 207
zusätzliche Parameter für das Servlet 221
Secure Access-Parameter
character-encoding 212
directory-servlet 223
filter-name 211
httpport 214
logdir 217
loglevel 216
logname 217
pathfrom 212

pathto 212
pattern 222
profile 214
realm 218
redirect-dir 219
redirect-url 219
secure 214
servlet 222
servlet-name 211
setcontentlength 223
translator 225
url-pattern 220
usepath 213
viphost 214
vippport
214
welcome-file-list 224
Seiten
Standard-Erweiterung festlegen 80
Server
Arbeitsspeicher 166
deinstallieren 130
Dienst einrichten 81, 100
Dienste entfernen 133
einrichten bei der Installation 97
hinzufügen 118
Kategorie bei Installation festlegen 100
starten 163
Startskripte 165
stoppen 169
Suchserver zuordnen 107
Serverkategorie 100
Service für Windows
entfernen 133
für Admin-Server 81
für WCM-Server 100
servlet (Secure Access-Parameter) 222
Servlet-Mapping
für Secure Access-Servlet 222
für Webanwendung 104
servlet-name (Secure Access-Parameter) 211
setcontentlength (Secure Access-Parameter) 223
Shared Pool (Oracle) 23
Sichere Verbindung
zum Content-Client 182, 184, 192
zum LDAP-Server 64
SMTP-Server
für Admin-Server 80
SQL Server 2000
JDBC-Treiber 83
Konfiguration 31
SSL
für Verbindung zum Content-Client 182, 184, 192
für Verbindung zum LDAP-Server 64
für WCM-Server 80, 99
Standardanwendung für Application-Server 103
Standard-Erweiterung für Seiten 80
Standardgruppen/-rollen für LDAP 38
Starten
Content-Server in Application-Server 170
Index-und Query-System separat (UNIX) 173
Installation über grafische Oberfläche 73
Installation über Konsole 160
Server 163
Suchserver 172
Startskripte der Server
Parameter 165
Stoppen
WCM-Server 169
substituteof (LDAP-Attribut) 54
Suchserver
deinstallieren 130

installieren 105
Server zuordnen 107
starten 172
Verzeichnisstruktur 129
Sun ONE Directory Server
Konfiguration 257

T

Tablespace
anlegen in Oracle 27
Tag Libraries
Verzeichnis 130
Taglib-Mapping
für Webanwendung 104
Tomcat
Konfiguration 180
translator (Secure Access-Parameter) 225
Truststore von Livelink WCM Server 64

U

Unicode
für Content-Client 99
für Secure Access 212
in Oracle einstellen 23
UNIX
Schreibrechte auf Verzeichnisse 126
Upgrade
der Datenhaltung (grafische Oberfläche) 231
der Datenhaltung (Konsole) 238
der WCM-Version (grafische Oberfläche) 228
der WCM-Version (Konsole) 236
Livelink WCM Server 227
Nacharbeiten 240
über grafische Oberfläche 227
über Konsole 236
url-pattern (Secure Access-Parameter) 220
usepath (Secure Access-Parameter) 213
UTF-8
für Content-Client 99
für Secure Access 212
in Oracle einstellen 23

V

Verzeichnis
für Installation 75
Verzeichnisse
nach der Installation 126
Schreibrechte 126
viphost (Secure Access-Parameter) 214
VIPP-Port 80, 98
vippport (Secure Access-Parameter) 214
virtueller Speicher 166
Voraussetzungen für die Installation von Livelink WCM Server 14
Vorkompilieren des Content-Clients 202

W

WCM-Server
Arbeitsspeicher 166
deinstallieren 130
Dienst einrichten 81, 100
Dienst entfernen 133
einrichten bei der Installation 97
hinzufügen 118
Kategorie bei Installation festlegen 100
starten 163
Startskripte 165
stoppen 169
Suchserver zuordnen 107

WCM-System
deinstallieren 130
WCM-Truststore 64
Webanwendung
erzeugen 101
Webserver
Konfiguration 177
Name für Secure Access angeben 214
welcome-file-list (Secure Access-Parameter) 224